



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

[ACM](#) Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 1

Monday 1 April 2002

Contents

- [ATF Takes Responsibility for Federal Software Policy Enforcement](#)
[ATFS Director](#)
- [REVIEW: "Hacking for Dummies", Bill Murray III/Gene Spafford](#)
[Rob Slade](#)
- [Computers to Cars](#)
[unknown source via PGN](#)
- [Surprise Settlement Evenly Splits Microsoft](#)
[unknown source via Gene Spafford](#)
- [Big security leak in Internet s*xshop](#)
[Paul van Keep](#)
- [Web site leaks customers address, offers extra discounts](#)
[Ron Gut](#)
- [Hackers find new way to bilk eBay users](#)
[Monty Solomon](#)
- [BT is publishing confidential ex-directory telephone numbers](#)
[Clive Jones](#)
- [Risks of using anti-spam blacklists](#)
[Eric Murray](#)
- [The smart highway](#)
[Raphael Lewis via Monty Solomon](#)

- [E-mail subscriptions, windows 2000 patches and photocopiers](#)
[Alistair McDonald](#)
 - [Re: Out with pilots, in with pibots](#)
[Robert Woodhead](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✈ ATF Takes Responsibility for Federal Software Policy Enforcement

<Director@ATFS.gov>

Mon, 1 Apr 2002 00:30:00 ET

WASHINGTON (Reuters) - The Department of the Treasury announced today that responsibility for enforcement of new federal regulations of the software industry will fall under the jurisdiction of the Bureau of Alcohol, Tobacco and Firearms (ATF). As the regulations come into effect, the bureau will be renamed to be the Bureau of Alcohol, Tobacco, Firearms, and Software (ATFS).

The new regulations have been taken by most observers as a key indication of the Federal Government's serious concern over the software production scandal gripping the nation. The final verdict of the grand jury investigation into the dangers of unregulated software production was praised as a major victory by software leaders in Redmond last month.

The grand jury investigation centered on the disturbing trend that key portions of the nation's critical infrastructure are being entrusted to a software product for which the secret inner workings (known as

`source
code') are becoming as prevalent as pornography on the Internet.

The Director of the ATF's 5,000-strong team of agents has pledged his full support to enforce the new regulations, under which all software development must take place only in licensed facilities by trained individuals. He was joined at a press conference this morning by the Director of the National Infrastructure Protection Center, who said, "It's about time the ATF took the entire software industry into its jurisdiction." He continued, "We would never consider laying the blueprints for our critical assets out for all to see. I applaud the new regulations for bringing sanity to a long unchecked industry."

The public will have until 1 Jun 2002 to dispose of all unregulated software products they may own. Possession of unlicensed software products can result in penalties up to 20 years in jail and multi-million dollar fines. Currently, only Smallsoft of Redmond, Washington, has achieved the necessary regulatory status to produce software in compliance with the new regulations.

An underground group of activists using the moniker ``the Electronic Frontier Foundation'' (EFF) has been strongly critical of the Federal Government's position throughout. Police have indicated the violent clashes are expected between supporters of the EFF and US Presidential nominee Billy Doors, the major proponent of the regulations, as he addresses business leaders in Winnemucca, Nevada, this afternoon.

[I suppose we can understand why they chose the acronym ATFS, given alternatives such as FATS, AFTS, FAST, etc. PGN]

REVIEW: "Hacking for Dummies", Bill Murray III/Gene Spafford

"Rob, grandpa of Ryan, Trevor, Devon & Hannah" <rslade@sprint.ca>
Mon, 1 Apr 2002 07:19:57 -0800

BKHAKDUM.RVW 20020401

"Hacking for Dummies", William Hugh Murray III/Eugene Spafford,
1802,
076455302X, U\$21.99/C\$437.84
%A William Hugh Murray III whmurray3@spryguy.com
%A Eugene Spafford spif@serious.purdue.edu
%C 155 Divet Road, Suite 310, San Mateo, CA 94402
%D 1902
%G 076455302X
%I International Data Group (IDG Books)
%O U\$21.99/C\$411.95 415-312-0650 fax: 415-286-2740
%P 166 p.
%S for Dummies
%T "Hacking for Dummies"

As regular RISKS readers will note, I always enjoy a new addition to the "for Dummies" series. This time the imprint has outdone itself with a lighthearted romp through network naughtiness, by two of the least known, but most accomplished, practitioners of the field.

Some may question the need for such a work, but the authors maintain that they are performing a valuable service to corporations and society at large.

"A vital system security penetration community is important," they state in

the introduction. "It thins the herd of security practitioners. We have a moral responsibility to ensure that those who, not having the authority to fire people who insist on using Outlook, get blamed when major events happen and are forced to look for work in other fields."

In a switch from the standard format, the "Part of Tens" comes first, pointing out how to knock holes in each of the ten domains of the security common body of knowledge. This sets up a series of helpful icons used to point out specific attacks that can be mounted against each domain.

(Security management attacks tend to get a bit repetitive after a while:

there are only so many ways of rewording the advice to pretend to be the CEO's secretary.)

Some common and handy attacks (such as the ubiquitous brute force denial-of-service attack, featuring a sledgehammer) are listed, but there are a number of little-known tricks, like the means of attacking a computer that has been sealed in a lead-lined vault, surrounded by armed guards, and cast in concrete. Dorothy Denning's sidebar on starting wars by manipulating e-mail systems is particularly interesting. Security professionals are not ignored: in an interesting display of fair-mindedness, the authors suggest that incident-response team members prepare by ensuring they always have plenty of sugar in their gas tanks for extra energy on late-night calls.

Critical reaction to the tome has been spirited but mixed. Winn Schwartau,

in the foreword, asks "is it moral, is it ethical" to provide such information to the general public, before concluding, "Who cares? Nobody has time for this." Phil Zimmermann has roundly condemned the section on anonymous communications, stating that the government has a legitimate need for access to private communications, while Fred Cohen is upset that the authors suggest viruses could be used for beneficial purposes. Richard Stallman is reported to be disturbed by the position that software development can take place in the kind of anarchic environment promoted by the book, and has launched a campaign to ensure that everyone has valid licenses for Microsoft products. Bruce Schneier, on the other hand, points out that the information in the book presents no danger to the public. "As long as you've got a strong crypto algorithm and good technical solutions, it doesn't matter about implementation and people."

copyright Robert M. Slade, 2002 BKHAKDUM.RVW 17020401
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

<http://victoria.tc.ca/techrev/~rslade> or <http://sun.soci.niu.edu/~rslade>

✶ Computers to Cars (unknown source)

Peter Neumann <risks@sri.com>

Mon, 1 Apr 2002

[I have had several requests for including this item in RISKS

from those

who have not yet seen it, even though it has been circulating for a while.

I have no idea who originally created it, but I am grateful to the author

for his or her incisive observations. PGN]

For all of us who feel only the deepest love and affection for the way computers have enhanced our lives:

At a recent computer exposition (COMDEX), Bill Gates reportedly compared the computer industry with the auto industry and stated: "If General Motors had kept up with the technology like the computer industry has, we would all be driving \$25.00 cars that got 1,000 miles to the gallon."

In response to Bill's comments, GM issued a press release stating: "If General Motors had developed technology like Microsoft, we would all be driving cars with the following characteristics:

1. For no reason whatsoever, your car would crash twice a day.
2. Every time they repainted the lines in the road, you would have to buy a new car.
3. Occasionally your car would die on the freeway for no reason. You would have to pull over to the side of the road, close all of the windows, shut off the car, restart it, and reopen the windows before you could continue. For some reason, you would simply accept this.
4. Occasionally, executing a maneuver such as a left turn would cause your car to shut down and refuse to restart, in which case you would have to reinstall the engine.

5. Macintosh would make a car that was powered by the sun, was reliable, five times as fast and twice as easy to drive -- but would run on only five percent of the roads.
6. The oil, water temperature, and alternator warning lights would all be replaced by a single "General Protection Fault" warning light.
7. The airbag system would ask "Are you sure?" before deploying.
8. Occasionally, for no reason whatsoever, your car would lock you out and refuse to let you in until you simultaneously lifted the door handle, turned the key and grabbed hold of the radio antenna.
9. Every time GM introduced a new car, car buyers would have to learn to drive all over again because none of the controls would operate in the same manner as the old car.
10. You'd have to press the "Start" button to turn the engine off.

🔥 Surprise Settlement Evenly Splits Microsoft (unknown source)

Gene Spafford <spaf@cerias.purdue.edu>

Mon, 21 Jan 2002 23:07:30 -0500

[From SatireWire, via various intermediaries. Reprinted for the occasion. PGN]

Decision Keeps Redmond from Monopolizing Massive Microsoft Patch Industry

Surprise Settlement Evenly Splits Microsoft; One Firm To Make Software,
Other To Make Patches

Redmond, Wash. In a surprise settlement today with nine U.S. states, Microsoft agreed to be split into two independent companies -- one that will continue to make Microsoft operating systems, browsers, and server software, and another, potentially larger company that will make patches for Microsoft operating systems, browsers, and server software.

Critics immediately charged that the settlement -- which overrides a previous agreement with the U.S. Department of Justice -- does nothing to diminish Microsoft's standing as the world's most powerful software company. But industry analysts argued that providing patches for security holes in Microsoft programs is a major, untapped growth industry, and applauded the states for not allowing Redmond to control it.

"Just consider, Microsoft can make an operating system, such as Windows XP, and sell 200 million copies, but each one of those copies is going to need at least five patches to fix security holes, so that's 1 billion patches," said Gartner Group analyst Mitch Fershing. "That is an enormous, undeveloped market."

Microsoft employees seem to agree, as sources in Redmond described a "mad scramble" among staffers to position themselves for spots at the new company, called Patchsoft. Asked why people would want to leave Microsoft for a startup, the source said the answer was "really quite

simple."

"Everyone here is asking themselves, 'Do I want to be part of the problem, or part of the solution?'" he said.

But J.P. Morgan analyst Sherill Walk suspects another motive. "Considering the sheer number of patches we're talking about, I think the new company will become another monopoly, and I believe the people who've jumped ship very well know that."

"Nonsense. It's really all about consumer choice," responded Patchsoft's new co-CEOs, Bill Gates and Steve Ballmer.

But how will Patchsoft make money? Currently, Microsoft issues free patches for problems in Windows XP, SQL Server, Internet Explorer, Outlook, Windows 2000, Flight Simulator, Front Page, Windows Me, Media Player, Passport, NT Server, Windows 98, LAN Manager (for a complete list of MS software needing patches, see www.support.microsoft.com). Under the agreement, Microsoft will no longer issue patches, which Gates said explains the recent five-day outage at Microsoft's upgrade site. "That was planned," he said. "It was a test of the Microsoft No Patch Access system. Went perfectly. No one was able to download anything."

At a press conference to outline the settlement, Connecticut Attorney General Richard Blumenthal pledged to keep a close eye on Patchsoft to ensure it would not overcharge for its services. He also expressed hope that other firms would soon become Certified Microsoft Patch

Developers

(CMPDs) and challenge the spin-off. Asked if Patchsoft, with so many former Microsoft employees, will have an advantage over potential competitors in the Microsoft patch market, Blumenthal said the settlement prohibits collaboration.

"Patchsoft developers will not have any foreknowledge of bugs or security holes before software is released. They'll just have to be surprised," he said.

"So it will be just like it was when they were at Microsoft," he added.

One Reuters reporter, meanwhile, questioned the long-term viability of Patchsoft. "This seems like a logical split right now, but what if Microsoft's products improve to the extent that patches are needed less frequently, or perhaps not at all?" she asked.

"I'm sorry, I can only respond to serious questions," Blumenthal answered.

🔥 Big security leak in Internet s*xshop

Paul van Keep <paul@sumatra.nl>

Fri, 22 Mar 2002 21:56:08 +0100

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. <http://nu.nl/document?n=53855>

🔥 Web site leaks customers address, offers extra discounts

Ron Gut <rgut@aware.com>

Thu, 14 Mar 2002 18:43:34 -0500

Saab USA embarked on a direct-mail marketing campaign to sell its cars. To past and potential customers it sent postcards with a web site address and an ID number, promising a \$50 savings bond for test driving a new car or a \$500 discount on the purchase of one.

The ID numbers run consecutively, starting at 1 (though Saab's personnel took care to pad the numbers out with leading zeros to a certain length, which does not present a difficulty if one already has an ID number in hand). The web site asks for the ID and presents the surfer with the ID

holder's address and the choice of the two incentives. Once the surfer chooses which incentive to receive the web site presents a JPEG image which needs to be printed, brought to a dealer and stamped by a sales person for Saab to honor it.

Problem number one: it is very easy to print out both types of coupons, and receive more discounts on a new car than Saab likely intended (a financial RISK here).

Problem number two: as was already hinted at above, it is very easy to enter other valid IDs at the web site, and therefore collect the addresses of people Saab thinks are likely to want a new car (both a privacy RISK to the unwitting customers and financial and PR RISKS to Saab).

Problem number three: since those IDs have already been sent out, Saab cannot change them! The web site can be changed to request the customer's name, as printed on the post card, in addition to the ID. The state or municipality should not be relied upon, as it appears Saab assigned IDs to customers sequentially after sorting the list geographically, making that field easier to guess. RISK here -- fixing this problem in the design stage would have been simpler, cheaper and less embarrassing than after release.

Problem number four: I decided to be a good netizen and report this to the Saab webmasters. Alas, I was foiled by their very fancy web site. The "Contact Saab" web page presents a form, but in Netscape 4.7 on X Windows

the only field that I can actually edit is the "Subject" field -- I can't actually report this problem (thus compounding all of the above RISKS). The same version of Netscape on Windows displays the form just fine, as does IE. What is the source of the RISK here? Non-conformance to standards? I doubt conformance to web standards will solve every instance of such a problem since most of the popular browsers do not fully comply with those standards (Netscape 4.7 certainly does not).

⚡ Hackers find new way to bilk eBay users

Monty Solomon <monty@roscom.com>

Mon, 25 Mar 2002 22:26:02 -0500

Source: Troy Wolverton, CNET News.com, 25 Mar 2002

Someone other than Gloria Geary had access to the Washington artist's eBay account last week. Using Geary's user ID, the person set up an auction for an Intel Pentium computer chip. Not only that, but the person changed Geary's password so she could no longer access her own account-- or cancel the bogus auction. Geary, who discovered the auction Friday, was able to convince eBay to pull down the auction over the weekend, but not before suffering through a stressful day of worrying about how the auction would affect her legitimate listings.

<http://news.com.com/2100-1017-868278.html>

✶ BT is publishing confidential ex-directory telephone numbers

Clive Jones <clive-nospam-risks@nsict.org>

Thu, 21 Mar 2002 14:56:40 GMT

British Telecom offers, in the UK, a range of discounted telephone services to domestic subscribers under the name "BT Together". One of their exclusions under some such schemes is calls to ISPs.

Go to the following part of their Web site:

http://www.bt.com/together/isp_exclusion.jsp

...and follow the "click here to view the full list" link.

This purports to be a list of telephone numbers for ISPs. However, it has been very crudely assembled, and includes several (possibly many) telephone numbers that are actually confidential ex-directory dial-in numbers for various organisations. When I looked, the list contained 4960 numbers in total.

The potential for abuse (especially denial of service) is obvious.

I.T. managers in the UK should check whether their dial-in numbers appear on the list. If they do, they should urgently consider having the telephone number changed.

✶ Risks of using anti-spam blacklists

Eric Murray <ericm@lne.com>

Fri, 22 Mar 2002 11:43:17 -0800

In the last week I have run up against two different RISKS related to anti-spam blacklists. These lists have grown from the old MAPS RBL system and are now run by a number of people. ORDB lists 15 different blacklists run by 12 different people or organizations.

Background: I run a small network that supports my consulting business and a few mailing lists. I've been a Unix geek since 1985, I've run some very large networks, and I've been active in network security since 1991. I've used RBL and I distribute my own anti-spam freeware. I hate spam.

Last week I got some bounced mail from one of my lists-- the recipient system was rejecting it as "spam" and the error message pointed me to ORDB.org. I was surprised to see this since I'm not running an open relay and there's never been spam sent from my network.

At ORDB.org I discovered that while my network was not actually listed by ORDB itself, it was listed by blackholes.five-ten-sg.com which is somehow linked to ORDB. I followed their web sites' process for getting off the list, which is to send e-mail to the maintainer. He reported that my network range is within a block "owned" by Verio, and he was blocking all of Verio because of a particular spammer that Verio hasn't gotten rid of. I replied "all of Verio for one spammer? What about everyone else

who's not a
spammer? Couldn't you be more accurate with your list and not
list the
netblock I'm in (in reality owned by Meer, not Verio)?" His
answer: "Too
bad for you, you should move".

The RISK here is that in using a blacklist or a service that
checks many
blacklists, one might be blocking a lot more than spammers.
Blacklists
might not be following the policy that you think they are
following, and may
be blocking address ranges out of spite or laziness, not because
of actual
spam.

Yesterday I started getting bounces from another list
subscriber, the error
messages said that I was an "insecure site" according to ORBZ,
another
blacklist service. ORBZ was taken off the net yesterday due to
legal
threats. Evidently the software that makes the check treats
ORBZ as a
whitelist, and since it's not answering, is rejecting mail that
it shouldn't
reject. (the site in question doesn't have aliases for
postmaster, admin or
root, so I can't even notify them of their problem).

The RISK? Poorly written checks of blacklists can produce
unintended
results when the list fails.

The temptation to go all out to kill spam needs to be tempered
with the
realization that communication is what makes the Internet work.
If you
don't care how much real mail you reject in your drive to block
spam, then
simply turn off your mailer and you won't get any spam at all.

✶ The smart highway

Monty Solomon <monty@roscom.com>

Sun, 24 Mar 2002 18:28:57 -0500

Over budget, behind schedule, the big brain would allow instant communication between controllers and drivers - if and when it works

[...] Called the Integrated Project Control System, or IPCS, the Central Artery's electronic monitoring mechanism will constitute the nation's largest, most sophisticated, and most expensive system, allowing highway operators and engineers to respond in real-time to collisions, car fires, and traffic jams, with plenty of help from computers that will do much of the thinking for them. [...] Beneath the pavement, 1,500 magnetic 'loop detectors' will monitor the progress of each vehicle passing above to gauge traffic flow, determine if a car has suddenly stopped or dramatically slowed - which could mean there has been an accident - and provide traffic counts to aid in planning. While the loop detectors could easily detect a speeder, project officials insist that state troopers will not have access to the data. [...]

Source: Raphael Lewis, *The Boston Globe*, 24 Mar 2002

http://www.boston.com/dailyglobe2/083/metro/The_smart_highway+.shtml

✶ E-mail subscriptions, windows 2000 patches and photocopiers

Alistair McDonald <alistair@inrevo.com>

Mon, 18 Mar 2002 21:54:55 +0000

E-mail subscriptions

I was working on-site for a client and a manager forwarded an e-mail newsletter, pointing a virus warning out to us. At the bottom of the message was a link to a web page to manage his subscription. I accidentally clicked the link, and was surprised that I had full control, without password, of his personal details and newsletter preferences (English, French, German, plain text or HTML). Maybe a confirmation e-mail would be sent to him about changes, I didn't try, but even being able to view the information should be forbidden without authentication.

Windows 2000 bugs

One of the items in a newsletter I received recently was this Microsoft knowledgebase article listing all the knowledgebase articles (bug reports, clarifications, and similar) about windows 2000 since the release of service pack 2 (released late 2001). There are currently 663 articles. No, make that 714, more have been added in the last 6 hours. Not all are bugs, but some are, and some are pretty serious too, for example Q265296: "Toshiba PC Card Controller May Power 3.3-Volt R2 PC Card at 5 Volts."

<http://support.microsoft.com/default.aspx?scid=%2Fsupport%2Fkb/q265296>

[2Fservicepacks%2Fwindows%2F2000%2Fwin2000%5Fpost%2Dsp2%5Fhotfixes%2Easp,](#)

[Apparently requires IE. PGN]

Photocopier stores document for later printing

While on-site at a client, I needed to copy a confidential document. I placed the document in the copier, and it complained about not having enough paper. I saw that another tray was full, so rotated my document (a lot of copiers auto-detect size and orientation) and tried again -- no joy. I filched some paper from a nearby laser printer, but instead of getting the two copies I ordered, I got six -- two from my first attempt, two from the second with the wrong orientation, and the last two once I'd rotated my document and tried again.

On investigation, the machine scans in a job even though there is no paper to fulfill it, and holds the documents in memory until there is. If I'd walked away to another photocopier, my confidential document would have been output whenever some kind-hearted soul replenished the paper, and when I was nowhere around.

- 1: Learn how to use all the tools you use, properly.
- 2: Assumptions don't carry from one device to the next, no matter how similar they seem.

Alistair McDonald

Inrevo Ltd

<http://www.inrevo.com/>

✈ Re: Out with pilots, in with pibots (Kristiansen, [RISKS-21.96](#))

Robert Woodhead <trebor@animeigo.com>

Fri, 15 Mar 2002 09:18:47 -0500

> [Gives me a nightmarish vision of a cloud of little unmanned
aircraft all
> heading for the same place, trying to avoid each other, ...

You see this happening every day. It is called a flock of birds, and the flocking algorithm is both very simple and works exceptionally well. They flow around obstructions like water.

In a proper flocking algorithm (which IIRC is basically "try to stay close to the center of the flock, but not too close to nearby birds") a foreign object passing through the flock would generate evasive maneuvers by nearby planes but the effects on more distant planes would be more and more diluted.

The reason a flock scatters is that the foreign object is often trying to eat a bird, at which point algorithm #2 ("It's every bird for himself") is activated.

Nevertheless, such innovations must be carefully scrutinized, as the possibility of a serious flockup is always present.



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

[ACM](#) Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 2

Thursday 4 April 2002

Contents

- [Announcing Immunix SnackGuard](#)
[Crispin Cowan](#)
- [Just because it's funny doesn't mean it isn't real](#)
[Donald A. Norman](#)
- [Re: Computers to Cars](#)
[David Harmon](#)
- [April Foolishness](#)
[PGN](#)
- [Real News on April 1st/KaZaA "leech" network](#)
[Nicholas C. Weaver](#)
- [IRS Form W-9095" -- that is NOT ISSUED by the Gov't](#)
[Jean Dugger](#)
- [When is fail-safe not fail-safe?](#)
[Phil Rose](#)
- [Barclays BACS payment system failure](#)
[Lindsay Marshall](#)
- [Gillette's Mach3 creates sales bonanza for thieves](#)
[Monty Solomon](#)
- [Yahoo Groups spam alert](#)
[John David Galt](#)

- [Yahoo users fume over "spam" switch](#)
[Monty Solomon](#)
 - [Re: UK ATC failure](#)
[Martyn Thomas](#)
 - [Re: Software "glitch" changes the colour of the universe](#)
[Douglas Siebert](#)
 - [Re: Loosing It's Grammer Skill's](#)
[Bruce Wampler](#)
 - [Re: The RISK of ignoring permission letters](#)
[Edward Reid](#)
 - [REVIEW: "Computer Forensics", Warren G. Kruse II/Jay G. Heiser](#)
[Rob Slade](#)
 - [Black Hat CFP](#)
[Jack Holleran](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✂ Announcing Immunix SnackGuard

Crispin Cowan <crispin@wirex.com>

Mon, 01 Apr 2002 08:54:41 -0800

New Product Release: SnackGuard
WireX Communications, Inc., 1 Apr 2002

[This arrived too late for the April Fool's Issue, but
better late than never? (Or better never than later?) PGN]

WireX is pleased to announce the latest addition to the Immunix family of security tools: SnackGuard. SnackGuard effectively guards your favorite snacks in the break room from "snack smashing" attacks: the predations of other hungry engineers. This protection is especially vital in these trying times of unemployment, when nomadic tribes of hunter/gatherer geeks roam the

halls of once mighty dot.com's in search of food and caffeine.

Following on StackGuard's "canary" defense, SnackGuard employs WireX's patent-pending "turkey" defense: when SnackGuard detects the "gobbling" noise of some turkey scarfing down your favorite pop tarts and heavily caffeinated beverages, it issues a pink slip, halting the gobbler.

While SnackGuard is effective in defending your snacks, it is not without costs. SnackGuard increases run time when you are running to catch the bus or the elevator, in that successful defense of your snacks tends to increase "programmer's butt". Excessive consumption of caffeinated beverages without intervening bathroom breaks may also induce personal "buffer overflows".

While SnackGuard is "free speech", it is not "free beer": you may modify and distribute this gag as you wish, but go buy your own brewskis.

Crispin Cowan, Ph.D., Chief Scientist, WireX Communications, Inc. <http://wirex.com> Security Hardened Linux Distribution <http://immunix.org>

✶ Just because it's funny doesn't mean it isn't real

"Donald A. Norman" <don@jnd.org>
Tue, 2 Apr 2002 18:13:06 -0600

In this year's April Fool edition, [RISKS-22.01](#), our fearless moderator reprinted that old item that purports to be from the auto

industry: if we made cars like computers, we'd always be crashing, rebooting, upgrading, ...

In particular, item 10 stated:

10. You'd have to press the "Start" button to turn the engine off.

Just because it's funny doesn't mean it's not real. The automobile industry is copying all the worst features of the computer industry, ignoring all the advances in user-interface design, and all the lessons about safety. I fear that someone in the industry a few years ago missed the significance of the date "April 1" in the United states. They took it seriously.

I point your attention to the new BMW Series 7 automobile. The key is simply a personal identifier that instructs the car to adjust the seat, mirrors, steering column, etc. to the key owner's preferences. To start the engine, push the "Start" button. To turn the engine off? Push the same "Start" button. That takes care of Pont number 10 in the "joke." (To be fair, the button is actually labeled START STOP, but then again, so too should the MS Windows button.)

But it gets worse. The New 7 series BMW no longer has all those knobs and buttons that clutter up the dashboard - you know, where each knob does one thing that you can count on. Instead, it has a single controller located on the center console that "functions similarly to a computer mouse." It drives a display in the center of the dashboard. It is called the iDrive: i for

"intuitive") (Don't get me started on intuitive. You know what's intuitive?

Fear of heights. Everything else we call intuitive, such as walking or using a pencil took years of practice. Is that what we want? A control that takes years of practice?)

The iDrive plus display, says the sales brochure, is a "user-friendly interface (that) offers quick access to over 700 settings, plus navigations system maps, phone book listings, and more" One control, one display -- 700 settings? What were they thinking?

As USA Today put it: "it manages to complicate simple functions beyond belief." Auto review said "iDrive is not simple, no matter how clean it looks to the naked eye. ... Our advice ... Is to ... retain basic manual controls for functions that are used every day.")

I work in the field of usability and safety. I am appalled. I do, however, have to keep an open mind. After all, I have not tested it. I did sit in the front seat in a showroom, but with everything turned off. I should drive it down the highway -- or better, a crowded city street - and test the iDrive. Set a new radio station, check the directions to my destination, see how much fuel I have left, adjust the temperature of the interior -- things I might actually do while driving. Only then can I pass judgment. Until then, I'm simply delighted that I am not planning to buy one. Alas, BMW promises that the features will migrate downward to all their autos.

Beware of April Fool jokes: they may come back to haunt you.

Don Norman, Computer Science, Northwestern University
Nielsen Norman Group norman@nngroup.com <http://www.jnd.org>

⚡ Re: Computers to Cars

David Harmon <source@netcom.com>

Thu, 04 Apr 2002 14:09:10 -0800

>6. The oil, water temperature, and alternator warning lights
would all be
>replaced by a single "General Protection Fault" warning light.

It's labeled "Check Engine". But opening the engine compartment
and
checking ("Yup, still there.") accomplishes little; instead you
need to
read some diagnostic code by plugging in a debugger that was not
furnished
when you bought the car.

⚡ April Foolishness

"Peter G. Neumann" <neumann@csl.sri.com>

Thu, 4 Apr 2002 12:21:17 PST

Quite a few people have apparently gone to Amazon.com to order
"Hacking For
Dummies" -- a bogus (i.e., nonexistent) book reviewed by Rob
Slade in
[RISKS-22.01](#). Perhaps, not surprisingly, the ISBN bears a strange
resemblance to the ISBN for "S*x for Dummies". We have to call
a Slade a

Slade. Perhaps his review was too subtle? Perhaps your fearless moderator needs to be more obvious in highlighting April Fools' items, besides putting it up front in the issue rather than buried in its usual end-of-the-issue position? Aw, come on! April Fool's Day is seemingly a worldwide tradition, and that's part of the fun.

🔥 Real News on April Fool's Day: KaZaA "leech" network

"Nicholas C. Weaver" <nweaver@CS.Berkeley.EDU>

Wed, 3 Apr 2002 14:00:47 -0800 (PST)

As reported on 1 Apr 2002,

<http://news.com.com/2100-1023-873181.html>

Brilliant Digital has been distributing 2 programs with KaZaA [1], one of which allows 3D, animated banner ads (ala Flash for 3D), and the second being the framework for what can only be described as a "leech" peer to peer network: using unused bandwidth, storage, and processor cycles on client machines to do tasks like banner advertisement serving, distributed computation, and distributed storage.

The second program is not complete, but is basically a Trojan which can be woken up to create this network. Being on April 1st, it smelled like an April Fool's prank, just far enough out to be believable, but not quite right.

Unfortunately, this isn't a hoax, but is 100% true. Firstly, an

e-mail with the reporter confirms that this was based on an interview with the CEO (possibly a point of fraud) and the SEC filings (annual report, form 10KSB). One could believe that the reporter was hoaxed by the CEO, but the SEC filings are presumed to be accurate in such matters.

Reading the SEC filings

<http://biz.yahoo.com/e/020401/bde.html>

confirms that this is what they are doing and HAVE been doing: the Trojan has been and continues to be distributed as part of KaZaA "third party" software, and they plan on creating a distributed, secure, network for distributed storage, bandwidth, and computation using this Trojan. And by installing the 3rd party software, KaZaA users have already agreed to these terms and conditions.

What are the RISKS, let me count the ways:

1) Serious news being released on 1 Apr. This is actually a pretty BIG deal: this story should have real legs, the implications are pretty astounding. But apart from being posted on slashdot (and being largely dismissed as April 1st), and being mirrored on MSN, it doesn't seem to have spread beyond that.

2) Trojans being "legitimately" installed as part of various applications. And if this forms a distributed network upon activation, this is another huge security risk. [2]

3) That some company thinks it can do "secure" content delivery using

untrusted clients (not just untrusted, but rather hostily acquired). Secure storage is reasonable (encrypt everything, distributed copies) but still hard. Secure distributed computation is very hard (an open research area, outside some very select problems), and secure distribution of bandwidth (say, for add serving) is a total crack-pipe dream.

4) The unwavering acceptance of license agreements on the part of users (who are so conditioned to click "OK").

[1] KaZaA's business model is "we give the program free, but charge people to bundle mandatory/voluntary programs with our download".

[2] Peer To Peer networks are hideously vulnerable to both active worms (which can spread quickly using the inherent topology) and contagion worms (which masquerade as "normal" traffic). Be Afraid.
Be Very Afraid.

Nicholas C. Weaver <nweaver@cs.berkeley.edu>

✶ "IRS Form W-9095" -- that is NOT ISSUED by the Gov't (via Lindsay Marshall)

<Adam Shand>

Fri, 29 Mar 2002 00:29 -0000

Given the source of who sent this to me this is almost certainly legit.
Just be aware.

Adam.

- ----- Forwarded message -----

Date: Thu, 28 Mar 2002 17:52:30 -0500

Subject: "IRS Form W-9095" - that is NOT ISSUED by the Gov't

FYI....

I personally know the person who posted this information and she does work for the USSS. I have not seen the document yet so if you have any questions direct them to Jean Dugger directly.

-----Original Message-----

Sent: Thursday, March 28, 2002 3:57 PM

To: METROTECH-L@LISTSERV.CC.EMORY.EDU

Subject: "IRS Form W-9095" - that is NOT ISSUED by the Gov't

To - ALL METRO TECH MEMBERS (PARTICULAR INTEREST - BANK SECURITY)
Fm - Jean Dugger, U S Secret Service
SUBJ - IRS Form - not from the Government....

Just when you think you've heard it all....you find out you haven't!!

Today, we were notified by a bank security good friend of the USSS that a form "W-9095" is circulating - which was accompanied by a letter, looking much like an official letterhead of the bank, requesting their customer to complete the form and fax it back to phone #914-470-9245.

I'm sure you'll be surprised to learn that the form requested all kinds of personal identifier information - ie, name, DOB, SSN, address, phone, parents' names and mother's maiden name - just about everything you would need to set up shop doing identity fraud!!

Luckily, a customer of the bank brought the form into a branch, to turn

it in, and bank security was alerted.

The form, called an "Application Form For Certificate Status/
Ownership
For Withholding Tax", is quite a work of art - and I feel sure
that it
has been widely distributed - my concern is that it could be VERY
widespread - perhaps by some former employee(s) who could gain
access to
bank customer records base - and send out such a thing!

The form, official looking as it is, claims to be a "Department
of the
Treasury Internal Revenue Service" form - which it is NOT. I
have
forwarded this info to IRS Internal investigations to see if
they would
take a look at it.

I will bring copies to share at MetroPol Fraud next week! My
thought is
that someone worked way too hard on this form to limit it's
distribution
to even one bank's customers! BE AWARE!

The bank letter is signed "Monique Meeuws" - and smells a lot
like a
"419" letter scam!!

Please notify the U S Secret Service - me or Chad Laub, 404-331-
6111, if
you identify these forms circulating to your customers!!

For the info of credit union organizations - please feel free to
post
this message on your systems as well.

We are looking into this and trying to develop more
information. Please
call me if you have info. More details to follow!

Jean, USSS

⚡ When is fail-safe not fail-safe?

"Phil Rose" <pvrose@tality.com>

Thu, 4 Apr 2002 11:40:16 +0100

Authorities are trying to restore order at a maximum security jail after an electrical storm led to the failure of cell locks.

<http://news.bbc.co.uk/go/em/-/hi/english/uk/scotland/newsid_1910000/1910131.stm>

A lightning strike destroyed an electricity sub-station supplying power to Shotts prison in Central Scotland, and the cell locks defaulted to what should be the fail-safe for electronic door locks - open. However should that be the case in a prison? Luckily for us who live close by the main prison security is still mechanical.

The risks - fail-safe modes must be carefully designed for the system application: don't rely on the component default fail-safe mode.

⚡ Barclays BACS payment system failure

"Lindsay Marshall" <Lindsay.Marshall@newcastle.ac.uk>

Sun, 31 Mar 2002 21:31:27 +0100

Barclays BACS payment system failed last week, and a large number of people did not get their pay check in their bank account. Normally this would not

be a huge problem, but because it is Easter and so has two bank holidays leading up to the last day of the month it is a huge disaster. I don't know the details of the software problem at all, but arrangements were made with banks to extend credit and Barclay's said they would pay any bank charges that anyone incurred because of not being paid. I am astonished that Pete Mellor hasn't sent you details. If you have a look on any of the UK newspaper sites for last week you will find something about it.

✶ Gillette's Mach3 creates sales bonanza for thieves

Monty Solomon <monty@roscom.com>

Sun, 31 Mar 2002 14:38:09 -0500

Razor burn:

Runaway popularity of Gillette's Mach3 creates a sales bonanza for thieves

Gillette is taking steps to stem the flow of stolen Mach3 products. Perhaps the most important, Szyal said, is a pioneering antitheft technology consortium at the Massachusetts Institute of Technology sponsored by Gillette, Procter and Gamble, and other large consumer-products companies. The MIT scientists are developing a microchip that, once embedded in the packaging of the Mach3 and other products, would allow the product to be tracked from factory to warehouse to retailer and everywhere in between. The chip, which began a one-year field test in Oklahoma in October, will allow

Gillette security officials to scan products for sale at a flea market and

determine where they came from. [Excerpt]

http://www.boston.com/dailyglobe2/089/business/Razor_burn+.shtml

⚡ Yahoo Groups spam alert

John David Galt <jdg@diogenes.sacramento.ca.us>

Sun, 31 Mar 2002 15:27:51 -0800

Yahoo has apparently made a sneaky change to the "Marketing Preferences" of all subscribers to mailing lists on yahoogroups.com, changing all their "No's" to "Yes". The result will be not only a load of spam, but also junk mail and even junk phone calls if your address or phone number are on file with Yahoo.

To change them back: Go to Yahoo Groups (<http://groups.yahoo.com>) and sign in. Go to My Groups and click on Account Info, verify your password if it asks you to, and your Yahoo ID card comes up. Click on 'Edit your Marketing Preferences' and change all those Yes's back to No's. Click Save Changes.

⚡ Yahoo users fume over "spam" switch

Monty Solomon <monty@roscom.com>

Sat, 30 Mar 2002 00:44:39 -0500

Yahoo users fume over "spam" switch, By Jim Hu, CNET News.com,
29 Mar 2002

Some Yahoo members on Friday reacted angrily to changes in the Web portal's e-mail marketing practices, comparing the company's revised policy to an open invitation to spam.

"I never received any notification about this from Yahoo," one annoyed reader wrote in an e-mail to CNET News.com. "I was merely lucky enough to have a friend warn me about it."

The ire stems from changes in Yahoo's "marketing preferences" page, which the company uses to secure permission to send service promotions. Along with other changes to the page, Yahoo said it had reset the default preferences for all members in a way that would require them to manually request that the company block the messages in the future--even if they had declined to accept such e-mail in the past. ...

<http://news.com.com/2100-1023-871730.html>

✶ Re: UK ATC failure

"Martyn Thomas" <martyn@thomas-associates.co.uk>
Fri, 29 Mar 2002 20:59:10 -0000

> ... this computer was not connected with the computers at...
Swanwick ATC
> ["connected with" is of course ambiguous in this context.

PGN-ed]

The failing system was the National Airspace System, NAS, according to press reports. This provides Flight Data Processing for Swanwick. "Connected to", rather than "connected with"?

Martyn Thomas, Holly Lawn, Prospect Place, Bath BA2 4QP 01225 335649

✶ Re: Software "glitch" changes the colour of the universe

Douglas Siebert <dsiebert@excisethis.khamsin.net>
Sat, 30 Mar 2002 20:19:21 +0000 (UTC)

(Mellor, [RISKS-21.98](#))

And since then they have announced that they weren't calculating it correctly (an algorithm error, as opposed to a software glitch) and that it is in fact salmon. I think its safe to say that these guys really have no idea what color the universe is. Looks mostly black to me, maybe I'm looking in the wrong direction :)

Douglas Siebert
khamsin.net

dsiebert@excisethis.

✶ Re: Loosing It's Grammer Skill's ([RISKS-21.94-96](#))

Bruce Wampler <bruce@objectcentral.com>
Fri, 29 Mar 2002 14:06:13 -0700

The current discussion on Spelling/Grammar prompts me to add some comments from my personal, first-hand perspective on the issue. I was the original developer of one of the first successful commercial grammar checkers - Grammatik. The major development of grammar checkers was at its peak in the late 1980's and early 1990's.

One of the most distressing things to me is the fact that the quality of both spelling and grammar checking software available today is no better than it was almost 10 years ago. How did this happen?

It may be hard to remember, but as recently as 1993 or 1994, you still had a real choice of what word processor you used. Today, Microsoft has a virtual monopoly with Word. In 1992, Microsoft decided that the state of grammar checking had gotten both good and essential enough that one should be integrated with Word. This decision has had many effects on the state of grammar checking.

In 1992, there were at least four grammar checkers available that could be considered state of the art, or nearly so. Microsoft chose one, and WordPerfect followed their lead by acquiring my company. The other companies faded into oblivion, with the ultimate result that, after a couple of years, there was no major new R&D going on with English grammar checking (to the best of my knowledge).

Because of this chain of events, the grammar checker you get today in Word

is not significantly better than the grammar checker you might have used almost 10 years ago. This is really sad because we were making great improvements in the quality and accuracy of the software, and had the development continued, there is little doubt that many of the deficiencies of grammar checking would have been overcome.

Unfortunately, as long as Microsoft considers the current grammar checking good enough, and as long as Word remains the dominant word processor, there will be little or no incentive for anyone to independently develop better grammar checkers. The RISK in this? Monopoly and complacency.

(This note has been spell checked, but not grammar checked. No grammar checking available for my e-mail software...)

Bruce E. Wampler, Ph.D., Author of the V C++ GUI Framework
bruce@objectcentral.com <http://www.objectcentral.com>

★ Re: The RISK of ignoring permission letters (Blaak, [RISKS-21.98](#))

Edward Reid <edward@paleo.org>
Sun, 31 Mar 2002 10:06:44 -0500

> Does this not have direct precedence with snail mail? I am
imagining CD
> clubs here. You can't be legally obligated by anything that
you receive in
> the mail and just throw away.

However, at least in the US it took legislation to establish the

principle that receipt of unsolicited merchandise incurs no obligation on the recipient. I think this occurred roughly 40 years ago, but I don't have a reference and a quick search on "unsolicited merchandise" makes it apparent that there are now many relevant laws.

Before such legislation was enacted, some merchants sent merchandise unsolicited and then dunned the unwilling recipients for payment unless they paid for return shipping. I don't know whether such merchants could actually collect in the face of determined opposition, but in most cases the individual recipient simply didn't have the resources to contest the bill.

If there's a lesson to be learned from the parallel between snail mail and e-mail, it's that individuals often need to be empowered by legislation to effectively resist commercial abuse.

REVIEW: "Computer Forensics", Warren G. Kruse II/Jay G. Heiser

Rob Slade <rslade@sprint.ca>
Tue, 26 Mar 2002 07:45:49 -0800

BKCMPFRN.RVW 20020221

"Computer Forensics", Warren G. Kruse II/Jay G. Heiser, 2001, 0-201-70719-5, U\$39.99/C\$59.95

%A Warren G. Kruse II wkruse@monmouth.com

%A Jay G. Heiser

%C P.O. Box 520, 26 Prince Andrew Place, Don Mills, Ontario

M3C 2T8

%D 2002

%G 0-201-70719-5

%I Addison-Wesley Publishing Co.

%O U\$39.99/C\$59.95 416-447-5101 fax: 416-443-0948 bkexpress@aw.com

%P 392 p.

%T "Computer Forensics: Incident Response Essentials"

I'm still disappointed that authors seem to think computer forensics is limited to data recovery, but this work at least has utility value going for it.

Chapter one is a rough outline of data recovery, with an emphasis on documentation and the chain of evidence. Basic information about IP addressing, for the purpose of tracing intruders, is given in chapter two:

it is useful and does not drown the reader in inconsequential details.

(There is an oddly vitriolic dismissal of the story of the origin of the term for Packet INternet Groper.) A valuable discussion of e-mail headers, and a very terse outline of intrusion detection systems (IDS) are also included. Hard drive basics and concepts are given in chapter three. The material is generally good, but some points on imaging and connecting are passed over rather quickly. Chapter four has a reasonable high-level overview of encryption abstractions, but it is difficult to see the immediate relevance of the material to forensics. "Data Hiding," chapter five, contains some meandering topics that range from password cracking to NTFS (NT File System) streams to steganography. A few tools for dealing

with these problems are listed. The description of hostile code, in chapter six, matches that of weeds in gardening: anything you don't want. It is, therefore, unsurprising to find that the content, while basically sound, is not particularly structured or helpful.

A list of software (and some hardware) tools are described in chapter seven. Chapter eight explains a number of points about the Windows operating system that might affect data recovery and forensics. (The material discussed is not, unfortunately, exhaustive, although it is very useful as far as it goes.) The introduction to UNIX, in chapter nine, is more structured and detailed, although it examines fewer specific tools. Chapter ten's general overview of an attack on a UNIX system is fairly standard, although there is a useful table of commonly compromised system utilities. A wide variety of tools and commands for collecting information from and about UNIX systems is given briefly in chapter eleven.

Chapter twelve is a short introduction to general concepts in the (US) law enforcement system. The last chapter is a rather abrupt finish to the book. There are seven appendices, the most useful of which is a handy point form overview of incident response activities.

Computer forensics books are starting to come out of the woodwork, and most offer such sage advice as "gather evidence" and "don't mess up the chain of custody." This book does tend to follow the same style and tone, but also has very valuable tips for practical work. It won't help you

much in
analysis, but it will help you become better at collecting data
that will
stand up in court.

copyright Robert M. Slade, 2002 BKCMPFRN.RVW 20020221
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

<http://victoria.tc.ca/techrev> or <http://sun.soci.niu.edu/~rslade>

⚡ Black Hat CFP

Jack Holleran <Holleran@severnapark.com>

Wed, 3 Apr 2002 13:17:21 -0500

Papers and presentations are now being accepted for the Black Hat Briefings 2002 conference. The conference is held from July 31-August 1, 2002 at the Caesars Palace Hotel and Resort in Las Vegas, NV, USA. Papers and requests to speak will be received and reviewed until May 1, 2002.

Please read the full announcement at:

<http://www.blackhat.com/html/bh-usa-02/bh-usa-02-cfp.html>



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

[ACM](#) Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 3

Monday 15 April 2002

Contents

- [Bank merger in Japan causes numerous problems](#)
[Jeremy Epstein](#)
- [Online banking system failure in a big way](#)
[Ishikawa](#)
- [Computer crime way up, says FBI](#)
[NewsScan](#)
- [Can you trust a "trusted traveler"?](#)
[NewsScan](#)
- [SMS, Net voting to be used in local UK elections in May](#)
[Anura Samara](#)
- [Patient overflow avoided: P1M, not Y2K](#)
[David Shaw](#)
- [More UK air traffic control failures](#)
[Mich Kabay](#)
- [Interface simplification](#)
[Devon McCormick](#)
- [Re: Just because it's funny doesn't mean it isn't real](#)
[Michael Walsh](#)
[Achim Nolcken Lohse](#)
- [Re: When is fail-safe not fail-safe?](#)

[Anthony W. Youngman](#)

● [Is your e-mail watching you?](#)

[Stefanie Olsen via Monty Solomon](#)

● [The Risks of using the wrong address](#)

[Dan Birchall](#)

● [Re: Yahoo Groups spam alert](#)

[Jim Horning](#)

● [Ray Bradbury's Fahrenheit 451, revisited](#)

[Marc Rotenberg](#)

● [REVIEW: "Hacker's Challenge", Mike Schiffman](#)

[Rob Slade](#)

● [Info on RISKS \(comp.risks\)](#)

✶ Bank merger in Japan causes numerous problems

"Jeremy Epstein" <jepstein@webmethods.com>

Mon, 8 Apr 2002 14:52:15 -0400

Three of the twelve largest banks in Japan merged. The results weren't pretty, including "more than 30,000 transaction errors and 2.5 million delayed debits" and "2.5 million of the 3 million automatic debits scheduled to be processed on 1 Apr 2002, including utility and credit card bills, couldn't be made on that day".

The problem was that each of the banks ran a different system (Hitachi, IBM, and Fujitsu, although no software was mentioned). They build some integration glue, but it didn't work.

http://www.computerworld.com/storyba/0,4125,NAV47_STO69943,00.html

✶ Online banking system failure in a big way

Ishikawa <ishikawa@yk.rim.or.jp>

Sat, 06 Apr 2002 18:16:32 +0900

This news seems to be reported over foreign wire services, and so may have been reported already but here it goes in any way.

Japan's Mizuho Financial group that operates the Mizuho Bank, which has been born out of the merger of three large banks, Dai-Ichi Kangyo bank, Nihon Kogyo bank, and Fuji bank, has started its merged new operation starting on 1 Apr 2002. (There is also another holding bank, but the Mizuho bank is the one where ordinary people have accounts carried over from the three banks.)

Since that day, the online banking transaction system of the new bank has been plagued with problems. On 1 Apr, the ATM malfunctioned and many users of the new bank could not withdrawal or deposit money. That continued until the next day.

I thought this was a labor pain often found in a new operation, but no the problem persisted and the cause seems to run much deeper than I originally thought.

Now for the last few days, the online banking transactions for payment of utility bills such as gas, electricity, water, and credit company payments are delayed heavily due to problems of unknown cause.

This morning's Asahi Shimbun newspaper (Yokohama edition) carried a top article that stated the management of Mizuho FG admitted the back log of transactions amounts to more than 2.5 million.

About three million such payments expected to take place on the 1 Apr could not be finished on time and 105,000 transactions remains unfinished even as of 5 Apr. The delay affected the subsequent processing of other transactions and the unfinished count exceeded 2.5 million on April 5th. (The fifth day of each month is the payment day of credit companies and thus there were many transactions to take place yesterday.)

About 30,000 incorrect double withdrawals, and about 5,000 double deposits were found and corrected. (Not all of them, it seems, to the evening NHK news I just heard.)

According to the bank, the current accumulation of delayed transaction would need the whole next week to finish.

The completion notification of utility bills payment to utility companies is also delayed very much. Such delayed notices are believed to be more than 5 million cases. (It seems as if the bank don't know exactly the status of the payment...)

The bank management admitted that although they have tested the integrated online transaction systems many times before the complete merger and the start of operation on 1 Apr, their expectation of the workload was not

accurate enough. (Above is my own translation.)

Since many Japanese companies have its fiscal year ends at the end of March, and starts a new fiscal year in April, the Monday being the first week day of April had more workload than expected according to the statement found in the newspaper article.

I noticed that the three banks closed the banking systems on Friday evening of the previous week and so I thought they took the time to move to the unified operation smoothly.

But, after the fact, some articles in newspapers suggested the previous testing period of the whole merger and unified operation was not long enough for the large scale operation at all. Also, there seems to have been a long period of discussion as to how the operations were to be unified and thus the implementation period became shorter than expected. Dai-ich Kangin used Fujitsu, Fuji used IBM, and Nihon Kogyo used Hitachi computers. The unified system seems to have been designed by Hitachi. The computers seem to be the mainframe UNIX types. As of now, it is not clear where/whether the problem lies in the integrated system hardware components and vendor supplied software or is in the application programmed by Mizuho.

I have an account at Dai-ichi and so is now a Mizuho customer. One solace is that the bank responded to the customer concern quickly and opened telephone hot line to track one's payment status, etc.. I have not tried the telephone number yet. The bank stated publicly it will cover

the cost incurred due to the delayed transactions. A big financial loss to the bank, I guess.

A failure in a spectacular manner. This will remain in Japanese banking history.

🔥 Computer crime way up, says FBI

"NewsScan" <newsscan@newsscan.com>

Mon, 08 Apr 2002 09:19:51 -0700

Eighty-five percent of respondents report having been victims of computer crime, costing them millions of dollars, according to a survey by the Computer Security Institute and the FBI. The study, which polled 583 computer security experts in business, government agencies, medical institutions and universities, concluded that the most serious losses stemmed from theft of proprietary information. In addition, almost all of the organizations had suffered from computer virus attacks last year, and 90% said they had been victims of Web site defacement in 2001, up from 64% a year earlier. "Organizations that want to survive in the coming years need to develop a comprehensive approach to information security, embracing both the human and technical dimensions," says Patrice Rapalus, director of the Computer Security Institute. In response to the growing threat of cybercrime, the FBI has set up the National Infrastructure Protection Center

and has formed regional Computer Intrusion Squads in several offices throughout the U.S. [BBC Online 8 Apr 2002; NewsScan Daily, 8 Apr 2002]
http://news.bbc.co.uk/hi/english/sci/tech/newsid_1916000/1916655.stm

✶ Can you trust a "trusted traveler"?

"NewsScan" <newsscan@newsscan.com>
Tue, 09 Apr 2002 09:32:41 -0700

One proposal for improving airport security has been the creation of hard-to-counterfeit "trusted traveler" ID cards for frequent travelers, but software developer Richard P. Eastman asks the obvious question: "What makes a trusted traveler? The guy who travels all the time; who travels on business; who has a reason to travel. Does that mean the terrorist can't penetrate that group? Of course he can." Beyond objections of that sort, civil libertarians have been arguing that ID cards for travelers will set a dangerous precedent. Barry S. Steinhardt of the American Civil Liberties Union predicts, "Quickly enough, policy makers are going to say, 'If this works, let's require everyone to go through background checks before they get on a plane.'" [*The New York Times*, 9 Apr 2002; NewsScan Daily, 9 Apr 2002]
<http://www.nytimes.com/2002/04/09/technology/09PASS.html>

✶ SMS, Net voting to be used in local UK elections in May

<Anura.Samara@facs.gov.au>

Wed, 10 Apr 2002 09:30:54 +1000

Local U.K. governments in Liverpool and Sheffield are gearing up to allow citizens to vote using SMS (Short Message Service) text messages and the Internet in elections 2 May 2002.

[<http://www.computerworld.com.au/idg2.nsf/All/E7E9EB212B30B99FCA256B960079B1B2!OpenDocument&NavArea=Home&SelectedCategoryName=News>]

✶ Patient overflow avoided: P1M, not Y2K

"David Shaw" <David.Shaw@itvworld.com>

Wed, 10 Apr 2002 09:00:22 +1000

The 2 Apr 2002 edition of *The Australian IT* (australiait.com.au) ran a story about the Royal Children's Hospital in Melbourne, Australia.

They've just finished upgrading their patient administration software. The software hasn't yet replaced the need for paper records but provides the foundation to do so. It uses a browser front-end.

Four years in the implementation, one of key drivers was the old software was unable to support patient numbers of more than six digits. The software went live on February 11. The 1,000,000th patient arrived in

March.

✈ More UK air traffic control failures

Mich Kabay <mkabay@compuserve.com>

Wed, 10 Apr 2002 08:50:06 -0400

On 10 Apr 2002 at 0605 BST, air-traffic control computers failed at the West

Drayton control center near Heathrow Airport, causing subsequent failures at

the control center in Swanwick, Hampshire. Disruptions lasted up to two

hours, with controllers working by hand to track planes.

According to a BBC

report [http://news.bbc.co.uk/1/hi/english/uk/](http://news.bbc.co.uk/1/hi/english/uk/newsid_1920000/1920527.stm)

[newsid_1920000/1920527.stm](http://news.bbc.co.uk/1/hi/english/uk/newsid_1920000/1920527.stm) this

is the second breakdown in ATC in Britain in two weeks.

Although the

current failure is being attributed to "creaky" old systems that are

unstable, the previous incident was attributed to a data-input error.

[Comments from MK: The comment on data-input error conveys a belief that

having a system crash because of incorrect inputs is understandable and

acceptable. It isn't. Good design includes edit checks on inputs,

especially inputs that can cause kernel panics. When there are forbidden

combinations of inputs, table-driven checks can exclude such combinations

before they are sent for further processing.]

M. E. Kabay, PhD, CISSP -- AssocProf Information Assurance

Dept CompInfoSys, Norwich University, Northfield VT

<http://www2.norwich.edu/mkabay/index.htm>

✶ Interface simplification (was Re: Computers to Cars)

Devon McCormick <devonmcc@yahoo.com>

Fri, 5 Apr 2002 09:17:35 -0800 (PST)

An example of the risk of "simplifying" an interface: while on vacation recently, I rented a new-model car. One reason I rented it was to take my daughter to a drive-in movie since these are rapidly disappearing and I wanted her to have this experience.

This drive-in, in Tucson, Arizona, does not have the speakers you attach to your car window. Instead, you tune your radio to a specified FM channel to get the sound for the movie.

As I started up the car to drive to the movie that night, I noticed that the headlights came on by themselves, presumably because it was dark out. We got to the movie, parked, found the radio station with the movie's soundtrack, and discovered that there is no way to turn off the headlights while keeping the power on to the radio!

One can imagine the (overly) clever engineer thinking "why would anyone want to sit in a car with the lights off and the power on?" Whereas some of us could come up with at least a couple of reasons for doing this, evidently Detroit isn't that imaginative.

Devon H. McCormick, CFA devon@acm.org

✶ Re: Just because it's funny doesn't mean it isn't real

Walsh Michael <michael.walsh@wmdata.fi>

Fri, 5 Apr 2002 11:50:44 +0300

Like Donald A. Norman, BMW's announcement of their intelligent 7 Series sent a shiver up my back.

In my case this was based on my experiences with an early version of one of their intelligent cars (a 1986 520 injection I was still using in 2001).

When BMW transferred (in connection with the Rover disaster) their dealership in Finland to a different company, they lost all expertise among their mechanics of the era before "computer-based" maintenance. This led to such funnies as my car refusing to start once in the middle of summer after a break of about 10 minutes in use; then me getting it to start after a couple of hours of leaving it alone and taking it to the dealership only to be told that by starting it it meant they were unable to download the details of why it went wrong.

What should I have done ? Bring it immediately next time the same thing happens. I then pointed out that this meant waiting to be stranded and getting a tow truck. Yes, they replied.

The very next day, that did in fact happen and I was towed all the way to the BMW dealership who then discovered that my model didn't have this download functionality as it was too old ...

You can perhaps see why relying on a BMW's intelligence is not appealing !

(A further funny was with the BMW extra I bought in Germany to enable me to pre-warm the car before using it. You set a clock in the car to the time this pre-warming should start (using petrol from the tank) and it warms the motor and inside of the car until you get into it. This worked perfectly when the temperature was around zero but at a few degrees less refused to click into action - not much use in Finland then. On the other hand at temperatures at around +25 degrees Centigrade it did jump into operation when you were driving along (and were in desperate need of more heat, NOT !!!)

Mike Walsh, Helsinki, Finland englantilainen@hotmail.com

✶ Re: Just because it's funny doesn't mean it isn't real ([RISKS-22.02](#))

"Achim Nolcken Lohse" <lohse@rockies.net>

Sat, 6 Apr 2002 02:00:59 -0700

Volkswagen has also thrown prudence to the winds in its rush to adopt high tech.

We bought a 2002 VW Golf earlier this year, and within a week, the alarm system malfunctioned. The first symptom was the unprovoked appearance of the "open door" icon on the dash. The next symptom was the sounding of the alarm some time after locking the car in the normal manner - ie. by clicking the remote or turning the key in the driver's lock.

The only way to prevent the alarm from going off was to lock the car manually, a procedure the misplaced confidence of the cars designers had made fiendishly difficult:

1. close the driver's door
2. lock all doors with remote
3. unlock the driver's door only with remote and reopen it
4. reach back to the rear door and unlock it with the handle latch
5. close the driver's door
6. open the rear door
7. reach forward from the rear and lock the front door by depressing the mechanical lock button
8. depress the mechanical lock button on the rear door and close it.

This is the only way to lock the car without arming the alarm.

Of course, the problem was intermittent. And the designers had not provided any diagnostics for the system. So on the first trip in to get the problem fixed, the dealership was unable to identify or solve it.

The solution had to wait until the problem had escalated to the

point where the hatchback could not be opened (in ANY manner! - there is no purely mechanical way to operate the hatchback latch). At this point the technicians' suspicion fell on the lock mechanism of the hatchback, which they then replaced, apparently fixing the problem.

The potential problems are actually worse than appears from above, as the car has only two keylocks, that in the driver's door, and the one in the hatchback. The hatchback lock (when it's working) can only be operated by the battery-operated master key (the valet key won't work on it). So it would seem that if you have only the valet key and the driver's lock jams, there's no way to get into the car, other than breaking a window.

Volkswagen supplies two of the master keys with the vehicle, and of these, the battery of one died in the first month. You're allowed to buy up to two more, but they cost more than CDN\$200 each!

✶ Re: When is fail-safe not fail-safe? (Rose, [RISKS-22.02](#))

"Anthony W. Youngman" <Anthony.Youngman@ECA-International.com>
Mon, 8 Apr 2002 11:46:50 +0100

> The risks -- fail-safe modes must be carefully designed for the system
> application: don't rely on the component default fail-safe mode.

Surely, for them to fail any other way would be life-threatening? Okay, the

prison needs an outer containment mechanism (and should have a backup generator), but if the power failed due to a fire within the prison, and all the doors failed locked, the prisoners would be trapped in their cells.

Given the design of those cells, death due to smoke inhalation could happen extremely quickly - from what I've seen typical design is cells opening onto walkways round a central "courtyard" - this would fill with lethal smoke in short order, should the fire be in the accommodation block. (And don't forget, many prisoners may well be "innocents" awaiting trial...)

Always think of the consequences of "safety" modifications. Like one incident I remember. An HSO demanded that a unprotected pulley belt be enclosed "for safety", despite the company concerned protesting most strongly that they'd never had anybody hurt, and it was a safety feature that it **wasn't** enclosed. Within months of doing as ordered, they'd had a serious accident, and the security housing was blamed in no uncertain terms as the cause of a minor incident turning into a major catastrophe. When one employee had an accident, his colleague had been unable to stop the machine by yanking the belt off the pulley, and by the time he'd run the length of the hall to the emergency stop button the trapped employee had been seriously injured.

⚡ Is your e-mail watching you?

Monty Solomon <monty@roscom.com>

Sat, 6 Apr 2002 15:39:42 -0500

[Stefanie Olsen, CNET News.com, 4 Apr 2002]

Watch out--the spam choking your e-mail in-box may be loaded with software that lets marketers track your moves online, and you may not even be aware that you've been bugged. Web sites have long planted bits of code called "cookies" on consumers' hard drives to tailor Internet pages for returning visitors and better target ads. Now, enhanced messages that share the look and feel of Web pages are being used to deliver the same bits of code through e-mail, in many cases without regard for safeguards that have been developed to protect consumer privacy on the Web.

"All of the security and privacy issues on the Web now relate to e-mail," said Adam Shostack, director of technology at Zero-Knowledge Systems, a Montreal-based privacy and security company. "The shame about this behavior is that it's going on surreptitiously and people are not given an obvious way to opt out." [...]

<http://news.com.com/2100-1023-875992.html>

✶ The Risks of using the wrong address

Dan Birchall <i_charge_100_bucks_per_spam@nospam.danbirchall.com>

10 Apr 2002 20:47:48 GMT

As a longtime spamfighter, I've learned to be a little careful about who gets my various e-mail addresses. If I wouldn't let someone call me collect... maybe they don't really deserve my personal e-mail address either.

As a longtime human, I make mistakes. A few months back, for example, I submitted a piece to RISKS from... my personal e-mail address. Whoops. Now it's available on the web at no fewer than 8 URLs.

Thus far, it's only gotten one piece of spam... I'll just hope other spammers and address-scraping 'bots are smart enough not to scrape addresses from a RISKS archive.

Dan (using the correct address this time)

✶ Re: Yahoo Groups spam alert ([RISKS-22.02](#))

Jim Horning <horning@intertrust.com>

Fri, 5 Apr 2002 14:24:09 -0800

Turns out you can't even log in to Yahoo to turn the options off unless you accept a cookie whose Compact Privacy Policy is unacceptable (to me, anyhow, your mileage may differ). At least I couldn't.

✶ Ray Bradbury's Fahrenheit 451, revisited

Marc Rotenberg <rotenberg@epic.org>

Thu, 11 Apr 2002 13:54:31 -0400

It seemed both appropriate and ironical to review Ray Bradbury's Fahrenheit 451 at this point in time. Earlier this month the US Congress began consideration of a bill that would ban the unauthorized reproduction of digital works. At almost the same time, federal prosecutors urged a court in Philadelphia to require technology in public libraries that would block access to information that some consider offensive.

There is no kerosene dripping from the pages of books in Washington or Philadelphia, but digital words would not burn. The methods of eradication must be more subtle, the technique more sophisticated.

It is tempting when reading Bradbury's classic work on censorship to draw parallels to book burnings from an earlier era, to make the obvious connection between the firemen in Bradbury's novel who set aflame houses that contained the printed word and those who gathered not so long ago to burn the words of Albert Einstein, Thomas Mann, Marcel Proust, Margaret Sanger, and H.G. Wells.

But Fahrenheit 451 is not simply about book burning. This is a world where the culture of censorship has permeated the public and the private. There is no intellectual life. There is no political life.

Interactive broadband technology provides endless entertainment through the full-screen images that appear on the walls of a parlor room. Words of meaning cannot be transmitted in any physical media.

They must be memorized and passed on as they were before the printing press, before the written word.

The protagonist Guy Montag, a fireman who will disavow his profession, confronts this reality in a series of encounters. First with a young woman who asks questions he cannot answer. Then with an old teacher who recalls a past that cannot be recorded. And finally with his boss, the Chief Firefighter who can quote Pope, Milton and Shaw, and then smile as a house and its contents are engulfed in flames.

Montag's future is not without hope. He will fare better than Orwell's Winston, Kafka's K, or the Prisoner before Dostoevsky's Grand Inquisitor. Still, the reconstruction of culture, literature, and history once recorded words are banished cannot be assumed. When a single person can recall only one essay of Thoreau's or a chapter from Bertrand Russell, the unique quality of information -- its ability to flow without bounds -- is effectively exterminated.

Perhaps it is unfair to compare the current legislative efforts to protect copyright interests or to prevent children from being exposed to images and words that are beyond their years with the unambiguous horror of burning a book because of the ideas contained inside. But technology does not make such distinctions, and capability creates opportunity. Already software filters have been turned on controversial ideas and unpopular organizations. And new copyright techniques will digitally incinerate recorded words that might otherwise be widely available.

In this year when many city mayors are urging residents to share the experience of reading a common book, Los Angeles Mayor Jim Hahn has

asked those in L.A. to read Fahrenheit 451. And Ray Bradbury's presence last week at a new mid-Wilshire bookstore, more than fifty years after the first publication of Fahrenheit 451, is a powerful reminder of the value of the written word.

Marc Rotenberg

<http://www.epic.org/bookstore/powells/redirect/alert907.html>

REVIEW: "Hacker's Challenge", Mike Schiffman

Rob Slade <rslade@sprint.ca>

Tue, 2 Apr 2002 08:32:57 -0800

BKHKRCHL.RVW 20020221

"Hacker's Challenge", Mike Schiffman, 2001, 0-07-219384-0, U
\$29.99

%A Mike Schiffman

%C 300 Water Street, Whitby, Ontario L1N 9B6

%D 2001

%G 0-07-219384-0

%I McGraw-Hill Ryerson/Osborne

%O U\$29.99 +1-800-565-5758 +1-905-430-5134 fax: 905-430-5020

%P 355 p.

%T "Hacker's Challenge"

Initially, I was skeptical of the title, considering the wording to be simply jumping on the current security bandwagon, with "hacker" this and "hacker" that on every bookshelf. In an odd way, however, the title is quite appropriate. This volume contains a series of twenty tests that are supposed to challenge your ability to analyze

network
data (most of the scenarios are network based) in order to
identify
and assess intrusions. Unfortunately, there are some problems
in the
implementation.

The book is divided into two parts. First come the twenty
scenarios,
with varying types and degrees of detail about the problems.
Then
come twenty "solutions," which are supposed to point out how you
should have approached the situation, and what indicators should
have
tipped you off to the intrusion and intruder. This physical
division
is rather meaningless: it isn't as if the solutions were short
phrases
that had to be printed upside down at the bottom of the page so
that
the reader doesn't inadvertently read the answer to the riddle
while
thinking about it. There is no reason that the solutions could
not
immediately follow the stories.

Actually, the pieces were written by thirteen different authors,
and
the amount of detail varies tremendously. Therefore, all the
possible
mistakes that could be made in a work of this type are
represented.
Sometimes the audit logs presented to us in the scenario contain
the
relevant details and very little else, but the explanation is
very
sparse. In other pieces readers are presented with huge amounts
of
log data, and the relevant points are lost. There are scenarios
which
are not complete, and the data necessary to solve the problem is
not
given until the solution write-up. A few pieces contain almost

no data for the reader in the problem section, while the solution presents almost no detection information or forensic exegesis. In one case we are given pages of log data and almost no analysis at all in the solution. There are articles that simply reproduce earlier situations with different characters. One solution makes no sense in terms of the data given in the problem outline. Some pieces are unclear, some simplistic, and some can only be described as misleading.

The occasional scenario is written up almost poetically, and isolated solutions do have tutelary explanations of how to read network audit logs.

If you are very good at forensic network analysis, you might enjoy pitting yourself against these challenges. Of course, if you are good at forensic network analysis you have more work than you can handle, and no time for games. If you are weak at network analysis, this book doesn't have very much to help you out.

copyright Robert M. Slade, 2002 BKHKRCHL.RVW 20020221
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

<http://victoria.tc.ca/techrev> or <http://sun.soci.niu.edu/~rslade>



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

[ACM](#) Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 4

Monday 22 April 2002

Contents

- [Y2K: The malady lingers on](#)
[Frank Carey](#)
- [Nanny-Cam may leave a home exposed](#)
[John Schwartz via Dave Farber](#)
- [Wireless used for water supplies](#)
[John R. McPherson](#)
- [More Web voting - UK local elections May 2002](#)
[R M Crorie](#)
- [Security flaw in Microsoft Office for Mac](#)
[Robert Lemos via Monty Solomon](#)
- [One-fourth of Mellon financial's I.T. work moved to India](#)
[NewsScan](#)
- [This is scary](#)
[Ted Lee](#)
- [Another April Fool's risk](#)
[Geoffrey Brent](#)
- [Citibank Visa woes](#)
[Bill Brykczynski](#)
- [Cracking for a fee](#)
[PGN](#)

- [CASPR Anti-virus Management and Protection discussion group](#)
[Rob Slade](#)
 - [Re: Computers to Cars, warning lights](#)
[Walter Underwood](#)
 - [REVIEW: "Handbook of Computer Crime Investigation", Eoghan Casey](#)
[Rob Slade](#)
 - [Conference on security information disclosure](#)
[Edward W. Felten](#)
 - [DSN 2002 Registration and Advance Program](#)
[Anup Ghosh](#)
 - [23RD ISODARCO SUMMER COURSE - Call for application](#)
[Diego Latella](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Y2K: The malady lingers on

Frank Carey <carey@voicenet.com>

Thu, 18 Apr 2002 21:02:08 -0400

Bugs fixed, cities must repay county over \$1M in erroneous disbursements

After two and a half years, Brevard County, Florida, has finally fixed the bugs that surfaced following installation of it's Y2K preparedness software in 1999. One bug prevented the county Clerk of Courts from determining how fines should be divided among the many cities and agencies that receive a share from each ticket. Since then, employees in the clerks office have estimated how big each city's checks should be. When new software became available last summer, the Clerk of Courts went through the records back to 1999 and discovered that some cities were significantly overpaid

and must

return the excess amounts. Melbourne owes \$430,993 and Cocoa owes \$353,083.

Melbourne Beach owes \$227,150, which represents about 10% of its budget.

City Manager William Hoskovec said: "We will have to make some concessions

or raise taxes...".

The Clerk of Courts office was unable to suspend drivers licenses because it

was impossible to track who was paying fines. Without the threat of license

suspension, many motorists didn't pay their fines and revenues from fines

dropped. With the bugs now fixed, notices are being sent to scofflaws and

the county expects to recover \$4 million for the cities to share, thus

reducing their reimbursement payments.

During the two and one half years of buggy software, the computers were

also blamed for issuance of incorrect bench warrants, mistaken judicial

assignments, failure to notify jurors of there summonses, and more.

Florida Today, 12 Apr 2002, front page

⚡ Nanny-Cam may leave a home exposed (John Schwartz, *NYTimes*)

Dave Farber <dave@farber.net>

Sat, 13 Apr 2002 20:41:57 -0400

Thousands of people who have installed a popular wireless video camera,

intending to increase the security of their homes and offices, have instead unknowingly opened a window on their activities to anyone equipped with a cheap receiver. The wireless video camera, which is heavily advertised on the Internet, is intended to send its video signal to a nearby base station, allowing it to be viewed on a computer or a television. But its signal can be intercepted from more than a quarter-mile away by off-the-shelf electronic equipment costing less than \$250. [...]

[Source: John Schwartz, *The New York Times*, 14 Apr 2002
<http://www.nytimes.com/2002/04/14/technology/14SPY.html?ex=1019744700&ei=1&en=cfeble93a276b9ee>]

From Dave's IP, <http://www.interesting-people.org/archives/interesting-people/>

Wireless used for water supplies

"John R. McPherson" <jrm21@cs.waikato.ac.nz>
Wed, 17 Apr 2002 21:42:35 +1200

... 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)
<http://www.nzherald.co.nz/storydisplay.cfm?>

[storyID=1392336&thesection=technology&thesubsection=general](#)

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.

✶ More Web voting - UK local elections May 2002

R M Crorie <robin@crorie.com>

Thu, 18 Apr 2002 23:15:11 +0100

I obtained some information about another Web voting trial, this time in the

UK, in Crewe & Nantwich Borough (Cheshire). This has been the subject of

fairly low-key advertising, perhaps because it is limited to two wards

(local electoral districts), Wybunbury and Maw Green.

However, it has been publicised as "e-mail voting", when in fact it is "Web

voting". Details are sketchy (local council officials are somewhat hesitant

about providing too much detail), but the company behind the trial is the

Oracle Corporation, in the form of Oracle (UK) Ltd.

Basically, the Council has posted a letter (actual snail mail) to every

eligible voter in these two wards with a "secret code". Over the next few

days, a second such letter, with another "secret code", will be sent,

together with a URL within the Council's Web domain

(www.crewe-nantwich.gov.uk), which will allow the voter to select their candidate and vote by entering the two previously-supplied codes.

The risks are pretty much as previously discussed in this forum for such

schemes, with the added irritation that only certain browsers are supported

- yes, it's IE and Netscape, but only the Windows versions, so tough cookie

to all you Linux-user voters out there - you have to turn up in person. It

looks like browser independence didn't feature highly in the design of the

trial, with only a vague reference to "security accreditation" being offered

as to why Linux browsers aren't acceptable.

That looks like a re-run of the UK Government Gateway browser-specificity

debacle - or the Microsoft Government Gateway, as we should call it now that

we have learned the Government has handed over the IPR for the whole thing

(£35m worth) to Microsoft completely free, on the basis of potential future

licence royalties... but that's another whole shed-load of risks...!

R M Crorie (risksANTISPAM-AT-REMOVEDcrorie.com)

✶ Security flaw in Microsoft Office for Mac (Robert Lemos)

Monty Solomon <monty@roscom.com>

Tue, 16 Apr 2002 22:33:24 -0400

By Robert Lemos, Staff Writer, CNET News.com, 16 Apr 2002

Microsoft acknowledged on Tuesday that its popular Office

applications for the Macintosh have a critical security flaw that leaves users' systems open to attack by worms and online vandals. The software slip-up happens because the Microsoft applications incorrectly handle the input to a certain HTML (Hypertext Markup Language) feature. By formatting a link in a particular manner, an attacker can cause a program to crash a Macintosh or run arbitrary commands. The link could appear on a Web page or in an HTML-enabled e-mail. [...] <http://news.com.com/2100-1001-884364.html>

✶ One-fourth of Mellon financial's I.T. work moved to India

"NewsScan" <newsscan@newsscan.com>

Wed, 17 Apr 2002 08:56:35 -0700

The latest financial giant to move much of its information technology work outside U.S. borders, Mellon Financial will soon be sending a quarter of its routine software maintenance chores to India. (A study by the Meta Group consulting firm indicates that an Indian programmer can be hired for one-fourteenth the rate of an American programmer.) Mellon executive Ken Herz says the company hopes to have new work for all U.S. workers affected by the company's decision, and explains: "This project emphasizes our intent to focus Mellon technology talent on growth-related projects and have routine maintenance work done offshore." (*San Jose Mercury News* 16 Apr

2002; NewsScan Daily, 17 April 2002)

<http://www.siliconvalley.com/mld/siliconvalley/3077722.htm>

⚡ This is scary

"Ted Lee, Minnetonka, MN" <Ted.Lee@udlp.com>

Fri, 05 Apr 2002 15:41:10 -0600

I had reason to question the denial of a claim on our dental insurance.

I called the appropriate 800 number and ended up choosing the menu item

for their "automated services." The first thing they asked for was my

subscriber identification number, which the voice then said "is usually

your social security number." I punched it in. The voice repeated it

back to me -- and then went on to spell out my name (yes, they had it

correct; OK, no middle initials, but first and last name were fine)

and give my birthdate. Need I say more?

⚡ Another April Fool's risk

Geoffrey Brent <g.brent@student.unsw.edu.au>

Tue, 16 Apr 2002 23:44:00 +1000

I run an e-mail discussion list for postgrad students at University of New

South Wales. At the beginning of 2001 UNSW moved to an on-line re-enrollment

system. Besides the obligatory teething problems, the designers

seemed to have forgotten that not all students were undergrads. Much of the information on the site, while good for undergrads, was quite misleading and confusing for the rest of us, leading to a good deal of frustration and venting on the list. (And at the end of the day, we **still** had to queue up to get our student cards, like always...)

One day after the last day of March, somebody <cough> 'forwarded' a message from a Mrs. Avril Fuller, announcing that all enrollment data had been lost in a server crash and that students would have to line up to re-re-enroll. Also, that they'd have to bring proof that they'd paid their fees first time around. Also, that their student numbers had been lost in the crash, and they'd be given new ones strictly by alphabetical order. (Note that the student number is printed on the cards everybody still had from when they re-enrolled.) Also, that because our e-mail accounts are based on student numbers, we would have to change addresses immediately.

In the previous weeks I'd been working hard to educate list members on 'how to spot a hoax', since I was tired of seeing supposedly-educated people sharing yet another variation of the Good Times warning every couple of weeks. I made sure Mrs. Fuller's message covered some of the biggies, like lack of date or any contact details for 'Mrs Fuller' beyond a non-existent e-mail address. And just in case anybody **still** didn't realise it was a joke, I also added that UNSW would be imposing a \$5 additional charge on each student to cover the costs of the extra work for their

staff.

Most of the list members got the joke, either immediately or (in one case) just before leaping from the top of the refrigerator to an untimely death. One, however, was completely taken in, and became very angry at University management.

When he realised it was a joke, he became even angrier at having demonstrated his gullibility in front of five hundred people, and directed that anger at me. Within a few weeks his behaviour forced me to eject him from the list, by which time he'd progressed to making quite serious threats against my person.

The (April Fool-specific) risks: Forgetting that there will ALWAYS be somebody who doesn't get the joke, no matter how obvious you make it - and that human failure modes are just as bizarre and dangerous as technological ones. Geoffrey Brent - g.brent@student.unsw.edu.au

Citibank Visa woes

Bill Brykczynski <bryk@software.org>
Fri, 5 Apr 2002 08:28:44 -0500

I usually pay my Citibank Visa bill via the Web, having the balance debited from my checking account. I tried to pay the bill the other morning, but this resulted in "We've had a problem processing your request. A general system error has occurred. Try your request again and let us

know if this problem continues." A repeated attempt resulted in the same message. So, I called them on the phone to inquire about the problem.

The person who answered the phone said hello from Citibank but did not ask for my account number (as is usual). So, I said "Good morning. May I provide you with my account number?" He said "No, our systems are down for maintenance. They should be up in a couple of hours." Ah, I said, that is why I cannot pay be the Web. Right, he said.

Unfortunately, over the next few days, I still could not pay via the Web. So, I called to pay by phone. The Citibank employee said they were having problems with their Web system. I said I would like to pay by phone. No problem said she. She asked for the last four digits of my checking account. Then she asked for a check number. After an immediate internal chuckle, I said "I'm paying by phone. Why do you need a check number?" "She said "We have to have a check number. You need to void that check number." I suspect that if I told her I was ROTFLMAO she would not chuckle at that, either. Anyway, I said "But there is no check! How can I give you a check number?" "We need a check number" was the best answer I got. So I said "I have a big problem with this. I do not want to pay my account balance by phone today. Thanks".

In retrospect, I should have given them a check number like "83750595828437693093". Or maybe a negative number. Or one with alphanumeric characters (imagine the fun I could have had with that

one ..."AMEXNo1").

The RISKS? Seems to me like I should be informed when there is a lengthy outage in the Web interface, instead of receiving a general error message. When I did contact them, the employee concurred with my assumption that the source of my problem was due to system maintenance. Apparently, he did not know about the extended Web problem. Having employees ask for a fictitious check number seems to be a poor procedure or suggests a lack of training. However, it was good for a chuckle. This time.

⚡ Cracking for a fee

"Peter G. Neumann" <neumann@csl.sri.com>

Fri, 5 Apr 2002 10:07:37 PST

A group of Chicago Web site operators say they will break into school, government and corporate computers and alter records, for fees starting at \$850. But at least one security expert thinks the operation probably is a scam. Among the services promised by Chicago-based 69 Hacking Services, is changing bad grades and other records on elementary, high school or college computer systems. [Source: Brian McWilliams, Newsbytes, <http://www.newsbytes.com/news/02/>]

⚡ CASPR Anti-virus Management and Protection discussion group

Rob Slade <rslade@sprint.ca>
Fri, 5 Apr 2002 12:53:23 -0800

Somebody recently pointed me to CASPR, the Commonly Accepted Security Practices and Recommendations group (www.caspr.org), loosely associated with ISC2 (www.isc2.org). They are looking for group leaders to lead groups in order to prepare papers on a variety (about 70) of security topics roughly grouped under the ten CBK domains.

I have created a Yahoo group for the Anti-virus Management and Protection topic, notified the CASPR people, and have apparently been accepted as the group leader. I have used the name malware in order to be somewhat more inclusive in the discussion. (I note that in CASPR viruses come under Computer Operations, whereas they appear in Applications Development in the ISC2 domains.)

The group name is CASPRmalware. To join, send e-mail to:
CASPRmalware-subscribe@yahoogroups.com

or see the group home page:

<http://groups.yahoo.com/group/CASPRmalware>

The group e-mail address is:

CASPRmalware@yahoogroups.com

This group is for discussion and preparation of the CASPR (<http://www.caspr.org>, Commonly Accepted Security Practices and Recommendations) Anti-virus Management and Protection document.

Currently membership is open and the discussion is unmoderated. I reserve the right to change that if circumstances warrant :-)

If any of you are interested, I would be delighted to have you

join.

rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

<http://victoria.tc.ca/techrev> or <http://sun.soci.niu.edu/~rslade>

[What might be a precursor effort that grew out of the
National Research

Council *Computers at Risk* study report led to The Generally
Accepted

Systems Security Principles:

<http://web.mit.edu/security/www/gassp1.html>

PGN]

✶ Re: Computers to Cars, warning lights ([RISKS-22.01-03](#))

Walter Underwood <wunder@inktomi.com>

Mon, 15 Apr 2002 16:49:51 -0700

This item:

6. The oil, water temperature, and alternator warning lights
would all be
replaced by a single "General Protection Fault" warning light.

is a much simplified version of an older, sarcastic comment on
the "ed"
editor's single warning message:

Brian Kernighan has an automobile which he helped design.
Unlike most automobiles, it has neither speedometer, nor gas
gauge, nor
any of the numerous idiot lights which plague the modern
driver.

Rather, if the driver makes any mistake, a giant "?" lights up
in the
center of the dashboard. "The experienced driver", he says,

"will
usually know what's wrong."

Sorry, I've lost the identity of the author, though it was
already in some
"fortune" files in 1983.

The worst consequence of this warning messages was when a user
tried to quit
without saving. "ed" would respond "?", and most users would
think, I said
"q", and repeat the command, losing all their work. To make
matters worse,
the system console was often a printing terminal, so someone
trying to
repair a system in single user mode was faced with a line-mode
editor which
they didn't know well, and which wouldn't give them useful
warnings.

Walter Underwood, wunder@inktomi.com, Senior Staff Engineer,
Inktomi
<http://www.inktomi.com/>

★ REVIEW: "Handbook of Computer Crime Investigation", Eoghan Casey

Rob Slade <rslade@sprint.ca>
Mon, 15 Apr 2002 07:35:25 -0800

BKCMCRIN.RVW 20020315

"Handbook of Computer Crime Investigation", Eoghan Casey, 2002,
0-12-163103-6

%E Eoghan Casey

%C 525 B Street, Suite 1900, San Diego, CA 92101-4495

%D 2002

%G 0-12-163103-6

%I Academic Press/Academic Press Professional/Harcourt Brace
%O U\$39.95 800-321-5068 fax: 619-699-6380 dtrujillo@acad.com
%P 448 p.
%T "Handbook of Computer Crime Investigation"

This book is hard to read. Not because of excessive technical rigour

or depth: quite the opposite. The work lacks focus and direction, and

appears to be a compilation of components without an assembly diagram.

It's the type of material that might result from the "war stories"

told around a security seminar, after the core curriculum had been

taken away.

Chapter one is entitled "Introduction," but, other than a statement

that the book is supposed to be a resource for forensic examiners who

may have to deal with computerized systems, there is almost no declaration of what the volume is about. The remaining material in

the chapter, while it does have an obvious relation to the act of obtaining evidence from computers, does not have any clear structure.

The points asserted are good advice, but appear to be relatively random thoughts. The text is neither readable nor lucid: in places it

seems more like a parody of obfuscated academic papers. Chapter two

is somewhat more understandable, offering an outline on how to prepare

documentation for discovery. Unfortunately, while it does deal with

some technical issues (original media is better than a bit-wise copy,

which is better than a copy of a file), the material concentrates on

lawyerly debates about what might be needed, and, after a great deal

of verbiage, boils down to the recommendation to produce all

possible

documentation, but not too much. (Where the material does get technical it frequently goes too far, starting to deal with specific pieces of software, rather than concepts.)

Part one looks at tools in forensic computing. Unfortunately, to a greater or lesser extent, the four chapters each deal only with a single tool or vendor; EnCase, Cisco's NetFlow logs, Network Flight Recorder, and NTI.

Part two is entitled technology: it looks at operating systems, networks, and other system types. Chapter seven provides some details of the FAT (File Allocation Table) and NTFS (NT File System) structures, as well as print spool files. A miscellaneous collection of information about UNIX files is given in chapter eight. A similarly unstructured compilation is listed in chapter nine, which reviews network data. Wireless network analysis, in chapter ten, concentrates on cellular telephone systems, and really only throws out generic information about such setups. Chapter eleven's overview of embedded systems varies between a similar generality and unhelpful photographs of breadboarded circuits.

Part three provides three case studies. While interesting (parts of the third are especially amusing), they really don't provide much in the way of assistance to anyone having to perform investigations.

The authors and contributors seem to be much more involved in the law, and law enforcement, than in the technology of computer forensics.

The book has no framework or structure within which to place the many

details. Therefore, the material simply blends into a haze of trivia, rather than providing the promised handbook. For those seriously working in the field there are many helpful points of information, but organizing them is left as an exercise to the reader.

copyright Robert M. Slade, 2002 BKCMCRIN.RVW 20020315
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

<http://victoria.tc.ca/techrev> or <http://sun.soci.niu.edu/~rslade>

Conference on security information disclosure

"Edward W. Felten" <ed@felten.com>

Mon, 22 Apr 2002 09:33:45 -0700

Conference on Cyber Security and Disclosure
May 9 at Stanford University

<http://www.seeuthere.com/rsvp/invitation/invitation.asp?CC=4%2F22%2F200209%3A25&id=/951771153071>

Stanford Law School Center for Internet & Society presents a conference

exploring the relationship between computer security, and disclosure of

information about security vulnerabilities. One view is that vulnerability

information should be kept secret and out of the hands of potential

criminals and foreign agents. Another view is that network administrators

require distributed research and public disclosure of vulnerability

information to enable them to secure their own systems.

Panelists will

discuss vulnerability disclosure and the trade-offs between

security,
government and corporate interests, and the public's right to
know. Computer
security researchers and practitioners, computer science
academics and
professionals, hackers, policy formulators, and private and
governmental
organizations concerned with securing private and public computer
infrastructures are invited to attend the conference.

This program is cosponsored by the Stanford Program in Law,
Science &
Technology and the Information Technology Association of America
(ITAA).

⚡ DSN 2002 Registration and Advance Program

Anup Ghosh <aghosh@darpa.mil>
Tue, 16 Apr 2002 14:39:09 -0400

2002 International Conference of Dependable Systems and
Networks: DSN 2002

Hyatt Regency, Bethesda, MD, 23-26 June 2002

The advance program, registration and accommodation information
are now
available at www.dsn.org. The early registration deadline is May
24, 2002.

This year's keynote speaker is the Honorable Richard Russell,
Associate
Director (Designate), White House Office of Science and
Technology Policy
(OSTP).

⚡ 23RD ISODARCO SUMMER COURSE - Call for application

Diego Latella <diego.latella@cnuce.cnr.it>

Fri, 12 Apr 2002 10:26:26 +0200

23rd SUMMER COURSE TRENTO - ITALY 3-13 AUGUST, 2002:

CYBERWAR, NETWAR AND THE REVOLUTION IN MILITARY AFFAIRS:
REAL THREATS AND VIRTUAL MYTHS

ISODARCO: INTERNATIONAL SCHOOL ON DISARMAMENT AND RESEARCH ON
CONFLICTS

Founded in 1966 (<http://www.isodarco.it>)

Sponsors: UNIVERSITY OF ROME "TOR VERGATA"; UNIVERSITY OF TRENTO;
ISTI - C.N.R., OPERA CAMPANA DEI CADUTI - Rovereto;
FORUM TARENTINO PER LA PACE - Autonomous Province of Trento;
U.S.P.I.D. - Section of Trento; Italian Pugwash Group

ISODARCO has been organizing residential courses on global security since 1966. The courses are intended for people already having a professional interest in the problems of disarmament and conflicts, or for those who would like to play a more active and technically competent role in this field. The courses have an interdisciplinary nature, and their subject matters extend from the technical and scientific side of the problems to their sociological and political implications. Cyberwar, Netwar and the Revolution in Military Affairs have given rise to a lively discussion in political and military circles in the last few years. Issues of major importance are: the relation between computers and regional defense; the threat of "cyberterrorism" as well as "cyberwar"; emerging forms of network organization and how information technology supports them; the impact of information technology developments in military doctrine and organization of

military forces. Of comparable importance is the issue of the possible implications on civil society and civil liberties possibly brought about by counter-measures to cyberwar and netwar.

[If you are interested, first read the full information at www.isodarco.it

This looks like a very interesting event. PGN]

Applications should arrive not later than June 3, 2002 and should be

addressed to the Director of the School:

Prof. CARLO SCHAERF, Department of Physics

University of Rome "Tor Vergata"

Via della Ricerca Scientifica 1, I-00133 Rome, Italy

Tel.: (+39) 06 72594560/1 -- Fax: (+39) 06 2040309

E-mail: isodarco@roma2.infn.it

The Course will be held at Istituto Salesiano "Maria Ausiliatrice",

Via Barbacovi 22, 38100 Trento, Italy. Tel. (+39) 0461 981265 and Fax

(+39) 0461 981972.

Directors of the Course: GARY CHAPMAN and DIEGO LATELLA

Dott. Diego Latella,

Consiglio Nazionale delle Ricerche

Area della Ricerca di Pisa - ISTI

Via G. Moruzzi, 1 - I56124 Pisa, ITALY

phone: +39 0503152982 or +39 348 8283101

fax: +39 0503138091 or +39 0503138092

e-mail: Diego.Latella@cnuce.cnr.it

<http://www.cnuce.pi.cnr.it/people/D.Latella>



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

[ACM](#) Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 5

Sunday 5 May 2002

Contents

- ["Don't Touch That Dial--Or You're Under Arrest!"](#)
[Lauren Weinstein](#)
- [Re: "Don't Touch That Dial--Or You're Under Arrest!"](#)
[Dan Gillmor](#)
- [Vivendi suspects electronic vote fraud](#)
[NewsScan](#)
- [Lost password' delays Mali vote count](#)
[PGN](#)
- [Online voting in UK](#)
[Toby Gottfried](#)
- [How to rig an election](#)
[*The Economist* via Mohammad Al-Ubaydli](#)
- [Seattle City light billing disputes](#)
[Jason Axley](#)
- [Risks of differing Unices](#)
[Theo Marketos](#)
- [CIA warns of Chinese plans for cyber-attacks on U.S.](#)
[Mike Hogsett](#)
- [Smart inventory control overshoot](#)
[Paul Breed](#)

- [California DMV online data base](#)
[Bruce Stein](#)
 - [A new risk to computers worldwide: W32/KLEZ.H" in MS Outlook](#)
[John Schwartz via John F. McMullen](#)
 - [How not to warn about viruses](#)
[Rob Slade](#)
 - [IE 6 Privacy features open users to attack](#)
[Monty Solomon](#)
 - [Midwest Express Web site security](#)
[Midwest Express](#)
 - [Robot cameras 'will predict crimes before they happen'](#)
[Merlyn Kline](#)
 - [Re: Online banking system failure in a big way](#)
[Ishikawa](#)
 - [Re: Nanny-Cam may leave a home exposed](#)
[Marc Roessler](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ "Don't Touch That Dial--Or You're Under Arrest!"

Lauren Weinstein <lauren@vortex.com>

Sun, 05 May 2002 14:51:01 -0700

Greetings. According to some in the entertainment industry, consumers risk becoming outlaws if they skip the commercials during television programs!

The latest Fact Squad Radio short audio segment concerns the escalating technology and political battle between the entertainment industry and their consumers, and is entitled:

"Don't Touch That Dial--Or You're Under Arrest!"

It's playable via:

<http://www.factsquad.org/radio>

Lauren Weinstein +1 (818) 225-2800

lauren@pfir.org or lauren@vortex.com or lauren@privacyforum.org

Co-Founder, PFIR, People For Internet Responsibility: <http://www.pfir.org/>

Fact Squad: <http://www.factsquad.org/> URIICA - Union for Representative

International Internet Cooperation and Analysis - <http://www.uriica.org>

Moderator, PRIVACY Forum - <http://www.vortex.com>

⚡ Re: "Don't Touch That Dial--Or You're Under Arrest!"

Dan Gillmor <dgillmor@sjmercury.com>

Sun, 05 May 2002 14:16:49

[From Dave Farber's IP, written in response to Dave's posting a notice from Lauren Weinstein similar to the above. PGN]

Dave, today's column [by Dan] is on point:

<http://www.siliconvalley.com/mld/siliconvalley/business/columnists/3200101.htm>

Dear Reader:

If you are reading this column in the newspaper, but did not read every article and look at every advertisement in previous sections, stop now. You must go back and look at all of that material before continuing with this column.

If you are reading this column on the Web and did not go to the

newspaper's
home page first, stop now. Go to the home page and navigate
through whatever
sequence of links our page designers have created to reach this
page, and
don't you dare fail to look at the ads.

Ridiculous? Of course.

Tell that to the dinosaurs at some major media and entertainment
companies.

They insist they have the right to tell you precisely how you
may use their
products.

[For IP archives see:

<http://www.interesting-people.org/archives/interesting-people/>]

✶ Vivendi suspects electronic vote fraud

"NewsScan" <newsscan@newsscan.com>

Mon, 29 Apr 2002 09:13:08 -0700

Vivendi Universal, the Paris-based media giant, is calling for a
criminal
investigation of suspected fraud by unnamed computer hackers
during a
shareholders vote by Internet last week. Vivendi thinks the vote
tampering

"could have been carried out by a small team armed with a
transmitter-
receiver and detailed knowledge of the procedures and technical
protocols of

electronic voting." (AP/*The Washington Post*, 29 Apr 2002;
NewsScan Daily,
29 Apr 2002)

[http://www.washingtonpost.com/wp-dyn/articles/A64981-2002Apr29.](http://www.washingtonpost.com/wp-dyn/articles/A64981-2002Apr29)

[html](#)

✂ **Lost password' delays Mali vote count**

"Peter G. Neumann" <neumann@csl.sri.com>

Tue, 30 Apr 2002 8:42:06 PDT

The announcement of the results of Mali's presidential election on 28 Apr 2002 has been suspended after a computer technician had a car accident, election officials have said. He is the only person with the password to access the election centre's computers. The technician was reportedly recovering in the hospital. [BBC, PGN-ed]

http://news.bbc.co.uk/hi/english/world/africa/newsid_1959000/1959327.stm

[... except that nobody wanted to admit how easy it might have been to break in without knowing the password, which would have blown the cover of the folks who had already rigged the election? PGN]
[This item was noted by several readers. TNX]

✂ **Online voting in UK**

"Toby Gottfried" <toby@gottfriedville.net>

Thu, 2 May 2002 15:51:53 -0700

Apparently the British are making moves toward voting in a "high tech" way.

And there are the worriers ...

<http://www.bbc.co.uk/webwise/column/col128.shtml>

<http://www.bbc.co.uk/webwise/column/col139.shtml>

"... But if there are unexpected results from next week's local elections in the UK it is entirely possible that they will be blamed on hackers, programming errors or network failures. The reason is that the May 2002 local elections are being used to test a selection of alternative voting methods. Most of these are 'e-voting' systems which use computers and networks, including the Internet. So if something unexpected happens there will be a temptation to blame it on the computers rather than take it as an reflection of a change in local opinion. ..."

Followup:

Quoting from the start and end of

<http://society.guardian.co.uk/modlocalgov/story/0,7999,645401,00.html>

which has links to more articles,

Residents of Sheffield and Liverpool will be able to vote over the

Internet and by mobile phone text message in the May local government

elections as part of a nationwide wave of 30 innovative electoral pilots

announced today. [Feb 5 2002]

The pilots will provide a crucial first test of Internet voting, and could

be a step towards an online general election. His announcement

came as the independent Electoral Reform Society (ERS) warned that the

government should not rush into online voting. Ministers need to ensure

the technology used is thoroughly tested and that tough safeguards are in place to prevent fraud.

✂ How to rig an election (*The Economist*)

"Dr Mohammad Al-Ubaydli" <mo@idiopathic.com>

Tue, 30 Apr 2002 15:00:27 -0400

[An article from *The Economist* print edition, 25 Apr 2002, considers a situation which readily generalizes to a state with N Congressional districts in which one redistricting gives results of N to 0 representatives one way, and another redistricting gives results of 1 to N-1 the other way.

Starkly PGN-ed from Dave Farber's IP

[http://www.interesting-people.org/archives/interesting-people/
http://www.economist.com/world/na/displayStory.cfm?
story_id=1099030](http://www.interesting-people.org/archives/interesting-people/http://www.economist.com/world/na/displayStory.cfm?story_id=1099030)]

✂ Seattle City light billing disputes

Jason Axley <jason-risks@axley.net>

Tue, 23 Apr 2002 11:33:02 -0700

Still no light has been shed on what is causing the massive overcharging of many Seattle City Light customers -- some as much as 10 times above normal.

Some quotes:

Seattle City Light, beleaguered by scores of customer complaints about inflated bills, now plans to do things "the Nordstrom way," meaning it will resolve billing disputes quickly and in the customer's favor when there's a question, Mayor Greg Nickels vowed yesterday.

The city made some headway in trying to turn around what has become a public-relations disaster. But after promising Friday to come up with a definitive explanation on the inflated bills for the mayor by Monday, it came up a bit short.

The hearing examiner "indicated that all my bills were from direct meter reads, so the bill in question was not a makeup bill," O'Leary said. "He also said the bill on its face was wrong. His conclusion was, however, that the meter never lies, and I must prove I did not use the power. How does one prove a negative?"

Zarker emphasized that the billing problem does not lie with the city's new \$40 million computer. "It works," he declared.

[Source: *Seattle Times*, "Nickels says City Light billing disputes will be resolved quickly, in customer's favor", 16 Apr 2002]
<http://archives.seattletimes.nwsourc.com/cgi-bin/teaxis.cgi/web/vortex/display?slug=citylight16m0&date=20020416>

Risks of differing Unices

Theo Markettos <theom@chiark.greenend.org.uk>

Tue, 30 Apr 2002 22:05:33 +0100 (BST)

Both Linux and HPUX provide a 'killall' command. Under Linux 'killall <process name>' is used to kill all processes with the given name -- for example, as root one might kill all instantiations of httpd.

Under HPUX, killall kills *every* process, except those required for shutdown. It takes an optional signal argument, but ignores this if it doesn't recognise it as a valid signal name. Hence 'killall httpd' kills everything except a handful of processes required for shutdown. If not running as root, it kills all processes owned by the current user.

The RISK? Don't assume something that is safe on one OS is on another, and don't assume that running a command without arguments to get help will do the right thing.

🚨 CIA warns of Chinese plans for cyber-attacks on U.S.

Mike Hogsett <hogsett@csl.sri.com>

Thu, 25 Apr 2002 14:07:50 -0700

U.S. intelligence officials believe the Chinese military is working to launch wide-scale cyber-attacks on American and Taiwanese computer networks, including Internet-linked military systems considered vulnerable to

sabotage, according to a classified CIA report.

<http://www.latimes.com/news/nationworld/world/la-042502china.story>

Smart inventory control overshoot

Paul Breed <Paul@Netburner.com>

Mon, 29 Apr 2002 14:15:16 -0700

I've been working on an old car, in the process of removing the spot welds I needed a specific sized bullet tipped drill bit. The bit would only last about 5 welds and I had hundreds to do. The only place I could find locally to buy the bits was in a pack of 15 various size bits at the local home center.

So, over the period of three months, I purchased all of their drill sets, every weekend (usually 3 sets). Now I have disassembled the old car and don't need more bits. The last time I was in the home center they had so many of these drill bit sets that they were overflowing on to the floor.

From my experience the computerized inventory system has a delay of about 3 months. It determined that this item sold out for 12 weeks straight, plugged this into it's inventory tracking prediction S/W and ordered hundreds and hundreds of sets.....

California DMV online data base

<Bruce Stein>

Wed, 24 Apr 2002 17:17:50 -0700

From the Los Angeles Times, 24 Apr 2002

<http://www.latimes.com/news/printedition/highway1/la-000028975apr24.story>

At the California DMV Web site at <http://www.smogcheck.ca.gov> ,
click on
"Vehicle Smog Check History". Enter just a license plate
number, and you
will be provided with:

Vehicle Identification Number (VIN)
Make, Model, and Year of the vehicle
The date and location of every smog test the vehicle has had.

The location of the smog test is almost always the neighborhood
where the
car lives.

In the case of Personalized License Plates, you get all of the
vehicles the
plate has ever been on.

A new risk to computers worldwide: W32/KLEZ.H" in MS Outlook

"John F. McMullen" <observer@westnet.com>

Sat, 27 Apr 2002 10:45:57 -0400 (EDT)

[Source: John Schwartz, *The New York Times*, 27 Apr 2002]

A rogue computer program that is the online equivalent of a

quick-change

artist is infecting computers around the world via e-mail and clogging

computer networks. The program, W32/KLEZ.H, is a "blended threat,"

combining elements of a virus, which infects machines, and a worm, which

transports itself from machine to machine. It also tries to disable some

antivirus programs. It makes itself hard for users to spot by changing its

e-mail subject line, message and name of the attachment at random, drawing

from a database that includes, for example, such subject lines as "Hello,

honey," and "A very funny Web site." The program has grown increasingly

common as users unknowingly activate it sometimes without even opening the

e-mail attachment that carries the virus and allow it to send copies of

itself to those in the victim's e-mail address file. [PGN-excerpted]

⚡ How not to warn about viruses

Rob Slade <rslade@sprint.ca>

Thu, 2 May 2002 10:28:11 -0800

The Klez family of viruses is not new: on the publicity page that I provide

at http://www.osborne.com/virus_alert/ I first warned of the family in

November of 2001. However, the author (or authors) has been continually

active, and some of the recent variants (particularly Klez.H) have been

successful enough that the virus warnings have been flying

around the net.

Unfortunately, not all of the warnings have been particularly helpful. Klez is one of the new breed of polymorphic e-mail viruses. Unlike Melissa, Loveletter, Hybris, or Sircam with their identifiable subject lines, attachment filenames, implied pornography, or ungrammatical message bodies, Klez variants present with a wide variety of subjects, bodies, filenames, topics, and (most recently) senders.

Recently I got my hands on what has to be one of the worst examples of a virus warning that I've ever seen:

```
> I have been advised that ther is a very bad computer virus
out. If opened
> the virus will attach itself to your address book.
>
> If you get an e-mail from W32.klez@jena.nn
>
> Do not open the attachment
>
> Delete it right away
```

I might note that, although I can't tell the source of this misinformation, it make several obvious errors. The attempt at a CARO virus name has a few problems: it doesn't have a variant designation (such as Klez.H), there appears to be some confusion with another extent virus (which makes mention of "Jenna"), and the "mass mailer" designation is usually .mm rather than .nn. More importantly, Klez does not have a consistent "From" indicator. Also, this particular company uses Microsoft Outlook for e-mail, and has no policy regarding the preview pane or other security related

configuration.

By the time anyone notices that an attachment exists, it will likely be too late.

(More recent Klez variants tend to pick a real e-mail address harvested from the infected computer to generate the "From" line in generated e-mail.

Therefore, those attempting to track infections will often concentrate on a machine or user that is not the source of the infection. I have heard from someone in another company who has been targeted by management as the source of the infection. This was interesting in that he was travelling at the time of the occurrence, and his computer was not connected to the Internet at all for a few days on either side of the event.)

For those interested in trying to detect Klez messages, three of the more reliable, but by no means universal, indicators are that, viewed manually, the MIME file type often does not match the filename extension, the filename extension is one of the usual executable crowd (.BAT, .PIF, .SCR, .EXE, etc.), and the size of the encoded file usually ranges between 120K and 180K.

(The old advice to avoid running attachments still holds true, albeit with a few provisos. Those who use Microsoft Outlook or Outlook Express may, because of the specialized construction of the message, still be at risk even if the attachment is not run deliberately run by the user. Due to this same construction, users of other mailers, such as Pegasus or Netscape

Communicator, may never see the attachment at all, and therefore may be at no risk.)

rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

<http://victoria.tc.ca/techrev/~rslade> or <http://sun.soci.niu.edu/~rslade>

⚡ IE 6 Privacy features open users to attack

Monty Solomon <monty@roscom.com>

Thu, 25 Apr 2002 02:13:41 -0400

By Brian McWilliams, *Newsbytes*, 23 Apr 2002

Security flaws in privacy features added to Microsoft's Web browser could enable attackers to perform several privacy-robbing attacks, including hijacking victims' MSN Messenger accounts, a security researcher warned.

According to Thor Larholm, a developer with Denmark-based Internet portal

Jubii.dk, "severe" bugs in the "Privacy Report" feature in Internet Explorer

version 6 can be exploited "in effect removing all privacy."

Last week,

Larholm posted an advisory and harmless demonstrations of the flaws at his

personal Web site. One example showed how the browser bugs enable a Web site

to launch programs that exist on the user's hard disk. Another demo page

silently sends a message to users in the target's MSN Messenger contact

list. ...

<http://www.newsbytes.com/news/02/176077.html>

✈ Midwest Express Web site security

<Midwest Express>

Fri, 26 Apr 2002 21:41:18 -0700

[via Mark Luntzel]

On the morning of Monday April 22, Midwest Express Airlines was informed that customer profile data had been published on the Internet, specifically on the U.S. Space and Naval Warfare Systems Command Web site. The data published contained a handful of user profiles including names and e-mail addresses. This screenshot of data was captured from the Midwest Express test server, not the actual Web site. This test server is used for testing new enhancements to www.midwestexpress.com.

Midwest Express has always taken steps to ensure security. As a result of this situation, a number of additional precautionary measures were taken to ensure that customer data was protected:

- * The U.S. Space and Naval Warfare Web site immediately removed the defaced Web page from the Internet.

- * A security company was contracted to eliminate any vulnerability to our test server.

- * All customer passwords to Web profiles were changed to protect and restrict access to the customer data.

Since all passwords have been changed, the next time you visit midwestexpress.com and login to your profile, you will be prompted to change your own password upon successfully answering a challenge/response question that you created.

While Midwest Express is confident in the security of its Web site, we are always assessing our Web site for potential vulnerabilities and taking appropriate steps when needed. We assure you that your customer information, purchases and other transactions are secure.

Tom Vick, Senior Vice President and Chief Marketing Officer

✶ Robot cameras 'will predict crimes before they happen'

"Merlyn Kline" <merlyn@zyweb.com>

Mon, 22 Apr 2002 13:36:51 +0100

According to the UK broadsheet **The Independent**, Dr Sergio Velastin, of Kingston University's Digital Imaging Research Centre, has developed software to analyse CCTV images for the purpose of predicting crime:

<http://news.independent.co.uk/uk/crime/story.jsp?story=287307>

Quote from the article:

Scientists at Kingston University in London have developed software able to anticipate if someone is about to mug an old lady or plant a bomb at an airport. It works by examining images coming in from close

circuit

television cameras (CCTV) and comparing them to behaviour patterns that

have already programmed into its memory. The software, called Cromatica,

can then mathematically work out what is likely to happen next. And if it

is likely to be a crime it can send a warning signal to a security guard

or police officer.

✉ **Re: Online banking system failure in a big way ([RISKS-22.03](#))**

Ishikawa <ishikawa@yk.rim.or.jp>

Sun, 21 Apr 2002 09:16:09 +0900

Here are a few interesting points to follow up the original story of online banking system failure of Japan's Mizuho bank.

It has been revealed that the Tokyo Electric utility which services the heavily populated Tokyo and its surrounding areas had asked the (soon-to-be) Mizuho bank for a dry-run of the utility bills payment before the merger back in February. The utility company was worried about the large scale change and requested that about 100,000 sample bills be run through the new integrated system to see if such bills are handled correctly. However, the bank turned down the request saying that their internal testing would be enough.

Obviously it was not!

The utility company requested the testing albeit the first refusal, but then again the request was turned down.

One of the reasons for the overload at the bank was mentioned as the failure of many transactions due to incorrect input data. It seems that the new integrated banking system required the conversion of old branch numbers of three banks into the newly assigned branch numbers. Some branch numbers were common among the three banks and they needed to be reassigned a new number once Mizuho bank went into operation. Apparently, some companies requesting the automatic billing failed to update the branch numbers in their transaction input (on MT!) and such transactions were deemed errors and manual intervention to inspect and rectify the aborted transactions were necessary.

Some of the double billings, etc. were attributed to the incorrect handling of magnetic tapes. Some tapes were obviously run through the system twice under the confused circumstances.

I think by failing to perform the 100,000 bills test run, the bank missed a great opportunity to test the integrated computer system and make sure the manual steps to intervene in case of failure is well organized and known to operation staff members.

There ARE now visible damages.

The utility companies (gas, electricity) and telephone companies can't figure out whether their bills were paid by the subscribers. The

amount of
money mentioned amounts to 25,000,000,000 yen. (That's
approximately US\$191
million at 1 dollar = 130.5 yen.)

Mizuho bank is negotiating with telephone companies and others
to pay an
agreed-upon ball-park sum of money, but since individual
transactions can't
be confirmed, the utility company can't figure out, say, if I
paid the bill,
so to speak. It seems that the utility companies decided to
send out BLANK
invoice notices without filling in the status of the payment
that were due
in April!) The utility companies are considering to ask the
bank to pay for
the additional cost to send complete receipts to their customers.

Small companies are hit hard when their payments didn't make it
on time due
to the banking failure. The small business associations all
over Japan
seemed to be flooded with complaints of their reputation being
on the line
due to the delay caused by the bank, not by their own failure.

I just heard a case of gas station owner whose salary payment to
part time
workers at the station failed to materialize in the worker's
account on TV
news.

This is getting serious.

In Japan, many companies have 25th as the monthly salary payment
day, and
since the long holiday weekend called Golden Week starts in
April 27, the
banking system will be busier. It is expected that many people
begin
withdrawing cash to use during the holidays and so the workload
on the

banking system is expected to soar due to the monthly salary payment, and the people taking out money from ATMs.

Since I am a customer of Mizuho, I have reason to concern...

With the revelation of the refusal to perform a dry run with the electric utility company to test the real world workload and a top management saying earlier at the parliament hearing about "No real harm was done to the customers", the Mizuho bank's reputation is all time low.

The Mizuho bank seems to think that their system can withstand the workload toward the end of the month, but who knows.

LATER-ADDED NOTE:

The bank has decided to stop ATMs all over Japan May 3rd and 4th, which are part of the holiday season. They had planned to operate ATMs during the holidays, but they deemed it necessary to stop the ATMs and check the banking system offline throughly.

⚡ Re: Nanny-Cam may leave a home exposed ([RISKS-22.04](#))

Marc Roessler <marc@tentacle.franken.de>
Tue, 23 Apr 2002 10:56:29 +0200

This is nothing new. Such cameras are even installed in some public restaurants and shops. Note that this basically voids all claims of the shop owners concerning privacy and data protection -- ANYONE can

receive that data. And, as more and more cameras are installed, the risk of malicious "camera takeovers" rises significantly. Think about webcams, cams integrated into notebooks/cellular phones, car dashboards (detect the driver falling asleep).. Those are easily tapped (or subverted, such as by installing trojan software/ firmware).. this has some enormous potential. The case of the Nanny-Cams shows the deviousness of this kind of attack: as the devices are not suspected to be used to spy on their owner ("I own that device; that makes it trusted"), they function more or less as hidden cameras. For more "camera takeover" scenarios take a look at my paper "How to find hidden cameras" [1].

[1] <http://www.franken.de/users/tentacle/papers/hiddencams.pdf>



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 6

Wednesday 8 May 2002

Contents

- [Unprepared for cyberattacks?](#)
[NewsScan](#)
- [Ashcroft wants stiffer penalties for identity theft](#)
[NewsScan](#)
- [The Console Buffer Knows...](#)
[Mark Bergman](#)
- [Salespionage](#)
[Rob Slade](#)
- [GNU in Not Unix](#)
[Dimitri Maziuk](#)
- [More on Clez](#)
[Rob Slade](#)
- [Moderated mailing lists and virus scanners](#)
[Matthew Byng-Maddick](#)
- [CLUTS: Composable Low-assurance UnTrusted Systems](#)
[Ben Laurie](#)
- [NRC report on porn](#)
[Herb Lin](#)
- [ACM invitation](#)
[Lillian Israel](#)

 [Info on RISKS \(comp.risks\)](http://comp.risks)

Unprepared for cyberattacks?

"NewsScan" <newsscan@newsscan.com>

Tue, 07 May 2002 09:01:12 -0700

People with knowledge of national intelligence briefings say that little has been done to protect the country against a cyberattack. Senator Jon Kyl (R-Ariz.) says: "It's a big threat, because it is easy to do and can cause great harm," and vulnerable U.S. targets are said to include the Centers for Disease Control and Prevention; FedWire, the money-movement clearing system maintained by the Federal Reserve Board; computer systems that operate water-treatment plants or that run electrical grids and dams; facilities that control the flow of information over the Internet; the nation's communications network, including telephone and 911 call centers; and air traffic control, rail and public transportation systems. Rep. Jane Harman (D-Calif.) says: "What I fear is the combination of a cyberattack coordinated with more traditional terrorism, undermining our ability to respond to an attack when lives are in danger." (USA Today 6 May 2002; NewsScan Daily, 7 May 2002)

<http://www.usatoday.com/life/cyber/tech/2002/05/06/cyber-terror.htm>

✶ Ashcroft wants stiffer penalties for identity theft

"NewsScan" <newsscan@newsscan.com>

Fri, 03 May 2002 08:20:55 -0700

U.S. Attorney General John D. Ashcroft is proposing legislation increasing by 2 to 5 years the jail time for persons convicted of aggravated identity theft a crime . "The Department of Justice is committed to seeing to it that criminals and terrorists cannot find refuge in the identities of law-abiding citizens of this country." Since October 1998, 2,223 criminal cases have been filed against 2,899 defendants. The call for tougher penalties won immediate support from Democrat Sen. Dianne Feinstein of California, who chairs the Senate Judiciary subcommittee on technology, terrorism and government. (*The Washington Post*, 3 May 2002; NewsScan Daily, 3 May 2002)

<http://www.washingtonpost.com/wp-dyn/articles/A24368-2002May2.html>

✶ The Console Buffer Knows...

Mark Bergman <risks@mercotech.com>

Mon, 06 May 2002 13:13:32 +0200

The advantage (and risk) of being able to use screen buffers and scroll bars to go "back in time" and see what happened in a terminal session is fairly well known, but I associate that kind of thing with fairly

"intelligent" GUI terminal emulators such as xterm. I happened to be using the "GSP" (Guardian Service Processor--a set of low level hardware and diagnostic routines) to check the cause of the blinking error LED on an HP "L" class server recently. I was using a very "dumb" console--just an 80x24 monitor and a keyboard with a serial connection to the server to access the GSP.

Among the dozens of commands within the GSP is a selection to show the console log.

I was pleased to see that the console log contained the many diagnostic messages that are displayed when the server boots up, before logins are available. I was also very surprised to find that the log also held the screen shots of the last console login session, including a telnet session into a network switch and the complete log (not just the commands, but all output as well) of the switch reconfiguration!

No passwords were visible this time, and this discovery isn't a particularly earth-shattering revelation. However, I think that there's a RISK when someone uses an apparently "dumb" device with no intrinsic "history" to connect to another device (the switch) with no command history, and yet there's a record of every screen preserved weeks later.

Mark Bergman

Salesponage

Rob Slade <rslade@sprint.ca>

Mon, 22 Apr 2002 19:50:21 -0800

Recently a RISKS reader has been regaling me with stories about life in the marketing trenches at--well, shall we just say A Very Large Technology Company.

AVLTC (TC to its very close friends), like most other technology companies, has a marketing arm. The marketing people have managed to include directives to be issued to all incoming staff. Prime among these is indoctrination about the importance of Contacts. Contacts, are, of course, the life blood of Sales and Marketing. Every Contact is to be forwarded to Marketing for inclusion in the database. And, in order for the Contact to be useful, it must include as much information about the Contact as possible. (Remember the old joke price list for Answers, Correct Answers, and so forth? Well, in the TC world, an Answer costs you a name, address, and phone number, while a Correct Answer costs you a life history. Even a Dumb Look costs you a name and phone number, at the very least.)

Since TC deals in Solutions (and don't we all?), many people approach TC speakers at conferences and seminars with Problems. In order to get a TC person to even listen to your Problem (hopefully thinking that they might get back to you with a Solution) you have to give them your Contact info. And that info goes into the database. And, of course, many of

the people
with the most interesting Problems might work for important
agencies. Like,
say, the military.

So TC has a Very Extensive List of names and phone numbers of
people in the
military, as well as other agencies.

Now, given the least benefit of the doubt, we can assume that TC
is not
interested in espionage. What TC *is* interested in is
Aggressive
Marketing. So they regularly have people call the numbers in
the List.
And, of course, if they have no other information, and if they
are worthy of
their Marketing headsets, they start asking questions.

In security realms this would be known as social engineering,
and it is a
really neat way to get people to tell you things that they
ordinarily
wouldn't. If you have the right number, and the right name,
there tends to
be a presumption that you also have the right to ask questions.
Particularly if you also know the right Problem.

But remember, this is not espionage, just Aggressive Marketing.

Now comes an interesting twist. Assume that TC has no interest
in
espionage. Assume that their Marketing and Sales people are all
of the
highest ethical calibre. (No, Peter, this is not a military
pun.) Even
granted all of this, TC does not use its own sales staff to
gather this
information. TC sales staff are highly trained and skilled
workers, and are
also paid more than three dollars per hour. So TC contracts out
this
information gathering work to outside companies. At this point,

unfortunately, the tale gets a bit fuzzy, since we don't know an awful lot about these companies, except that they are likely also the people who phone you at dinner time to sell excess credit cards and unwanted magazines.

Well, we do know slightly more about these companies. Said companies provide a valuable employment opportunity to any number of rather low paid workers who are very likely industrious and entrepreneurial. And, if the lack of command of the English language is any indication, also recent immigrants to these shores.

rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com
<http://victoria.tc.ca/techrev> or <http://sun.soci.niu.edu/~rslade>

GNU in Not Unix (Re: Markettos, [RISKS-22.05](#))

Dimitri Maziuk <dmaziuk@yola.bmrb.wisc.edu>
Mon, 6 May 2002 14:52:30 -0500

Well, that particular risk is well known to professional Unix systems administrators -- in fact, I was rather surprised to see that Linux "killall" made the RISKS now: it's been [in]famous among Unix sysadmins for quite a while now.

I see two issues here: one is that of false advertising, and another one -- of professionalism (not that they are entirely unrelated).

Stallman's rants about "LiGNUx" have a perfectly good technical reason behind them: "Linux" (as in "OS based on Linux kernel and free software") has lots of GNU software in it, and "GNU is Not Unix". Hence, Linux is *Not* Unix, regardless of what Linux advocates may be telling us, it is "GNU". (And, BTW, Unix is Not GNU.)

That was about false advertising, now let's look at professionalism.

Linux killall is perfect illustration of what happens when a product is designed by a dilettante.

Back in 1975 professionals designed an OS called Unix. Being professionals, they realised the need for certain design principles. Such as splitting a task into a number of smaller subtasks and designing a separate tool to handle each subtask (that does one thing, and does it well)[0].

For example, shutting down a computer involves flushing (synchronizing) file buffers to disk ("sync"), killing all running processes ("killall"), and powering off the machine ("poweroff", at least on Solaris). All perfectly neat and logical.

Along comes a layman who is unaware of the above principle, nor of the significant "prior art"[1]. Result? -- read Theo's message.

(Various observations to show that isn't such a big problem (in no particular order):

* professionals already know that similarly-named utilities often

behave differently on different operating systems,
* GNU folks never intended to uphold the aforementioned design principle in the first place (see EMACS), so no surprises there,
after all, you'll only run "killall" on a Unix once.)

We have a bigger problem with another Unix principle: source code portability.

As software becomes more complex, it requires more sophisticated build tools. More and more open source software is being developed using GNU compilers and build tools, and it is becoming dependant on them. The result?
-- While portability at the level of each compilation unit is still maintained, the whole thing is not portable anymore. It fails to build on non-GNU systems[2].

GNU project in particular did a great service to software community by promoting and popularizing free software. It also did a great disservice by turning the whole thing into a political issue, and pretty much ignoring the need for competence and expertise on the part of software developers. Instead of sound software engineering, we now have "Free Speech" flag-waving[3].

With more companies (individuals, governments) jumping on Linux bandwagon, the situation becomes eerily reminiscent of the recent dot-com boom; back then we had The Internet and e-words, now we have Open Source and Linux. Back then a few cautionary voices drowned in marketing hype, now they're likely to be branded Paid Advocates of Evil Entertainment Industry and Oppressors of Free Speech[tm] -- so they shut up and go learn Plan9, or

something.

(BTW, if it sounds like I'm singling GNU out, I'm not.

Microsoft

et al., did at least as much as GNU to get us where we are now. The whole thing would be very different if there was e.g. a liability clause in every software license.)

But the \$15 question remains: would you board an airplane designed by, say, 2nd year biology student as a night-time hobby? So what makes you think their software design skills are any better?

Hmm. This came out sounding like a rant. Well, it probably is.

Dima

[0] Various aspects of the problems related to complex software systems are very familiar to RISKS readers. They come up in, what? -- every other RISKS issue? 25+ years ago Unix authors were well aware of them, too.

[1] Irix and Solaris "killall", for example, behave like HP-UX one -- not surprising, considering the "grand scheme of things" outlined above.

[2] Anyone who ever tried building open source software on Solaris using native build tools knows that 9 times out of 10 GNU "libtool" fails to link shared libraries. The remaining 1 time GNU ./configure script fails to determine compiler flags to make position-independent code (needed for said libraries). And since GNU compiler and build tools are unable to produce 64-bit code on Solaris, the libraries, and all software that uses them must be built as 32-bit binaries. Now, why did I pay for that 64-bit hardware,

again?

[3] And instead of one Shakespeare, we have a zillion monkeys with C compilers. As history of Usenet shows, we shouldn't expect them to come up with even "Hello World" anytime soon, not to mention "Hamlet".

✶ More on Clez (Re: Slade, [RISKS-22.05](#))

Rob Slade <rslade@sprint.ca>
Tue, 7 May 2002 16:17:48 -0800

Crying Klez: Maybe the sky **is** falling
by Robert M. Slade

Maybe it's because the name is unassuming, without the flash of a "Melissa" or "Loveletter" or "Chernobyl." Maybe it's because various reports have called it Klaz, Kletz, W32/Klez.[a-k]@mm, or I-Worm. Klez. Maybe it's because the public's attention has been exhausted by media viruses like Code Red. Maybe it's because there have been a number of versions, and only the latest one has made an impact. Maybe it's because the beast is bewilderingly complicated.

Whatever the reason, a virus called Klez (or, more specifically, Klez.H) seems to be happily spreading far and wide, without much attention from anyone except antiviral vendors. Warnings have been issued about it, but these are often limited and unhelpful. The general media does not appear to have paid any attention to the problem at all. One of the most widespread and dangerous viruses of recent times, Klez is hard to identify, is difficult to track, is generating serious numbers, and carries a number of payloads.

Also,
it probably isn't the last of it's kind.

Klez is actually a family of viruses. The limited information available seems to indicate that the same author or a small group, probably resident in China, is likely responsible for all of the Klez variants. Eight have been identified so far, seemingly released between the fall of 2001 and spring of 2002. Each variant has added new features and payloads. In little over half a year the Klez family has gone from being a minor nuisance to a major threat.

The first version was so buggy that flaws in programming seemed to be the major concern. However, even then the virus was notable for its ambition and complexity. In addition to spreading itself, Klez dropped a virus called ElKern. (There have been reports of a new version of a new version of the CIH virus traveling with Klez, but this may be due to infection of the Klez program file itself.) The subject line, sender address, and filename attachment were all variable, avoiding the major means of e-mail virus detection. (Various Klez variant subject lines have promised games, humour, pornography, vague but important messages, and, interestingly, antiviral protection.) Klez also used a vulnerability in Microsoft's Outlook mailer (actually resident in Internet Explorer programming) that would automatically unpack and invoke the message attachment, in some cases before the message was even read by the user.

(This mailer loophole, sometimes known as the IFRAME vulnerability, had actually been addressed and patched by Microsoft in March of 2001.

Users who had regularly upgraded installed patches would not have been at risk of this specific function. The bug is addressed in www.microsoft.com/windows/ie/downloads/critical/q290108/default.asp and <http://www.microsoft.com/technet/security/bulletin/MS01-020.asp>.

However, the more widely known Microsoft security bulletin, <http://www.microsoft.com/technet/security/bulletin/MS01-027.asp>, deals with a composite patch, and talks about browser certificates, rather than the mail problem. It is also interesting to note that, in order to use this function, Klez forms messages with a non-standard MIME [Multimedia Internet Mail Extensions] format. Non-Microsoft mailers, such as Pegasus and Netscape Communicator, may not even allow users to see the attachment, and thus, inadvertently, offer users additional protection.)

The file attachment, as of version H, will have an extension of .EXE, .BAT, .PIF, or .SCR. The MIME file type will not match the extension (although that is not a reliable indicator of a virus infection). E-mail addresses used to create new infected messages are harvested from the infected machine. Recent versions of the virus also have code to use ICQ as a source of e-mail addresses.

Klez.E (version 2.0, according to internal text), released in January of 2002, added file infection capabilities, so that the virus could spread using e-mail, direct copying to network shares, and infection of program files. (Windows system files were often corrupted by the infection attempts. Other files might be infected by a

companion type

method: the original file was renamed and hidden and a copy of Klez written with the original filename.) The virus carried its own SMTP (Simple Mail Transfer Protocol) program so that it did not need to use local mail clients. The "From" line was also faked such that if Alice received an infected message from Bob, it might not come from Bob but from Charles, who had addresses for both Alice and Bob on his infected machine. This function not only prevented tracking of the infected machine, but caused many people to try and track infections in the wrong place. In addition, the virus had a payload to overwrite text, Microsoft Word, MP3, HTML and other files with random data, thus destroying the contents.

Early versions of the virus had a hidden message (in the body of the infected message) seemingly indicating that the author was trying to gain a reputation in order to get a better job. Later versions tried to kill processes of the Code Red family of worms, including Nimda, and included hidden messages suggesting that Klez was an antivirus virus. Klez.E, in addition to adding to the list of virus processes that would be stopped, also killed processes for a number of the most popular and effective antiviral programs. It would remove Windows Registry keys for antiviral software, and also corrupted checksums or deleted files for antiviral systems. (Text strings seemed to indicate that this was because the world had not offered the author a

well-
paying computer job.)

The latest version (as of this writing), Klez.H, often sends itself in a message offering a tool to remove and immunize against Klez.E. (It purports to come from one of a number of well-known antiviral companies.) Klez.H also added a new function: it would frequently pick up a file from the infected computer and add it as an attachment to the infected message sent out. There is already one known case where a confidential negotiating document was transmitted to a mailing list of several thousand people in this manner. Fortunately, the file overwriting payload seems to have been removed.

Any available virus tends to spawn variants. It is also not unusual for a virus author to improve on his (or her) own work, and release new versions. However, variants seldom involve additions of functions and features to the extent seen in Klez. The original version alone demonstrated effective social engineering and polymorphic techniques, as well as complex features that would be dangerous in conjunction with other forms of malware. In less than six months, the author (and the greatest probability is that there is a single author) has added features manipulating processes in memory, attacking antiviral and security software, increasing the means of reproduction and spread, and attacking data availability and confidentiality. It is unlikely that this is the last version of Klez that will be seen, and a

number

of common viruses could give the author new ideas for new payloads to add and new technologies to employ.

In a sense, though, there is absolutely nothing new about Klez. Microsoft software is well-known to be full of bugs and security loopholes: Internet Explorer is much more dangerous to use as a browser than is Netscape Navigator. There are dangerous technologies in common programs that should be disabled or patched. There is a definite trend towards convergence in malware, with different types of programs supporting and distributing each other. Polymorphism has long been known in file infecting viruses: the use of variant subject lines in Klez is tame compared to the (literally) myriad forms of files generated by Tremor.

Most importantly, however, your mother's old adage still holds true.

"DON'T RUN THAT PROGRAM ON YOUR COMPUTER! YOU DON'T KNOW WHERE IT'S BEEN!"

rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

<http://victoria.tc.ca/techrev> or <http://sun.soci.niu.edu/~rslade>

✶ Moderated mailing lists and virus scanners

Matthew Byng-Maddick <mbm@colondot.net>

Tue, 7 May 2002 14:12:46 +0100

Some readers of RISKS may be familiar with Dan Bernstein's ezmlm mailing

list manager, and some more may have used the slightly more full-featured ezmlm-idx. In both of these, extensive use is made of a cryptographically hashed input address, to confirm particular actions. In particular, it almost always sets these addresses as the e-mail "Reply-To:" header, so that when you just hit your "Reply" button in your user-agent, things work sanely.

The case of a moderated announce list managed by ezmlm-idx is no different. The moderation includes the full request (as with the rest of ezmlm), and a bit of text telling you how to moderate the message, and the "Reply-To:" header set. This would seem fine.

Now let us consider the case where the moderator has some kind of virus scanning, a not entirely uncommon case in this modern world, and that we have a virus which picks senders and recipients out of addresses in your address book.

The virus decides that it's going to send itself to the announce list. This should not be a problem, as the list is moderated, except, in this case, the message is included in its entirety at the bottom of the request for moderation. An online virus scanner, looking for signatures will decide (correctly) that there is a virus. It therefore replies to the sender of the message to tell them that there is a virus, but in this case, the virus software in question is slightly broken, and uses the From: and Reply-To: headers to work out where it should send the warning.

But, any
mail to the Reply-To: address will cause the held message to be
sent out
to the announcees.

So the only time the protection doesn't work is when there are
viruses,
arguably when it most needs it.

Of course, this doesn't just apply to viruses, but what happens
with
moderator "Out of office" autoreplies?

The RISKS:

Well, I can see several here

- * In the quest to make such things as moderation of a list
easier,
the MLM is using the Reply-To header so that all you need to
do
is reply to that virtual mailbox. There is no checking of,
say,
a subject line, or something that necessitates human input.
- * The virus scanner is non-compliant with the standards, and is
delivering an effective Delivery Status Notification message
(`We couldn't deliver your message because we believe it to
be
virus-infected.`) to address designated for user-agent
rather
than transport-agent use.
- * This case only occurs where the system sees a virus infected
file,
which is not a case that will be tested for when building the
system.
- * Sending out a virus to your customers via your announce list
is
probably unlikely to make you popular.

Matthew Byng-Maddick
colondot.net/

<mbm@colondot.net>

<http://>

CLUTS: Composable Low-assurance UnTrusted Systems

Ben Laurie <ben@algroup.co.uk>

Tue, 07 May 2002 14:10:47 +0100

ezmlm, when running a moderated mailing list, sends messages to the moderators with the From and Reply-To addresses set to cause rejection and acceptance of the moderated message, respectively.

If the moderators use certain virus scanning services that shall remain nameless, and a virus (such as the currently rampant Klez, which also forges the sender address, so is more likely to be accepted for moderation) is sent to the moderated list, those services report the virus to the Reply-To address (erroneously, IMO - these should be seen as delivery errors and reported to the Return-Path, see RFC 2821), causing the virus to be accepted and distributed to the list.

One RISK is obvious. The other, IMO, is poorly defined standards for e-mail that make it incredibly difficult to work out what the right thing to do is in these cases.

Incidentally, vacation(1) send to the From address, which will cause rejection - not such a bad outcome, but also wrong. But whose fault is the error?

<http://www.apache-ssl.org/ben.html>

<http://www.thebunker.>

[net/](#)

✶ NRC report on porn

"Herb Lin" <HLin@nas.edu>

Mon, 6 May 2002 01:34:43 -0400

Given RISKS readers' interest in these matters, the National Academies'

report entitled "Youth, Pornography and the Internet" was released on May 2.

The report examines approaches to protecting children and teens from

Internet pornography, threats from sexual predators operating online, and

other inappropriate material on the Internet. It discusses social and

educational strategies, technological tools, and policy options for how to

teach children to make safe and appropriate decisions about what they see

and experience on the Internet. Chaired by former Attorney General Dick

Thornburgh, it's the most comprehensive study yet on the topic.

More information on the report is available at:

<http://www4.nationalacademies.org/onpi/webextra.nsf/web/porn?OpenDocument>

The report itself is available online at:

http://bob.nap.edu/html/youth_internet/

If you are interested in a briefing on or discussions about the report, please

contact the study director, Herb Lin, at 202-334-3191.

ACM invitation

Lillian Israel <israel@hq.acm.org>

Tue, 7 May 2002 14:26:40 -0400

[The Risks Forum is an official ACM activity. Although we normally never run advertising in RISKS, perhaps we owe the ACM this one. PGN]

IT and computing professionals are invited to join ACM and receive a special 15% discount on their first-year membership, PLUS receive a FREE Limited-Edition IT book! A second free book is also available if you add a subscription to the optional ACM Portal (available at a 15% savings as well). ACM even has a special offer designed just for students!

To learn more, and to Join ACM now, go to:

<http://www.acm.org/joinacm1>

Some of the valuable benefits of an ACM membership include:

- * Full access to the Online Guide to Computing Literature (July 2002)
- * Free access to ACM's new Distance Learning Portal (July 2002) - 150+ online courses
- * A one-year subscription to "Communications of the ACM"
- * The option to subscribe to the enormous online ACM Portal - one of the world's largest databases of IT information and the ultimate resource for IT professionals!

Find out more about the many benefits of an ACM membership, and read about the FREE Limited Edition books at: <http://www.acm.org/joinacm1>

ACM, the Association for Computing Machinery, is the world's

leading

scientific and educational society serving the IT and Computing communities. Founded in 1947, ACM has members in more than 100 countries.



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

[ACM](#) Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 7

Saturday 18 May 2002

Contents

- [Apple Computer's hidden spam filtering](#)
[Derek K. Miller](#)
- [Apple: break your new PC with a copy-protected CD, it's not our fault](#)
[Charles Arthur via Dave Farber](#)
- [Shipping the Big Iron: a computer-related risk!](#)
[Mike Hogsett](#)
- [UK govt wants to make "e-filing" compulsory for taxes](#)
[David Cantrell](#)
- [Verisign doesn't encrypt credit-card info](#)
[Daniel Norton](#)
- [Making a list, checking it never](#)
[Adam Shostack](#)
- [Re: The Console Buffer Knows...](#)
[Dick Mills](#)
- [Re: GNU is not UNIX](#)
[Theodore Ts'o](#)
[Dimitri Maziuk](#)
- [More on Klez](#)
[Bob Morrell](#)
[Paul Mech](#)

● [Info on RISKS \(comp.risks\)](#)

✶ Apple Computer's hidden spam filtering

"Derek K. Miller" <dkmiller@pobox.com>

Thu, 9 May 2002 10:46:54 -0700

According to a recent report at the Mac-focused news site MacInTouch, Apple Computer places surreptitious spam filters on the free POP3/IMAP mac.com e-mail addresses it provides to Mac OS computer users.

<<http://www.macintouch.com/applemailfiltering.html>>

Apple does not advertise its filtering, does not reveal how it works, and provides no way to turn it off or adjust its parameters.

The risk is clear: spam filtering is far from perfect, and Apple's is no exception. It both lets through actual spam and rejects some legitimate mail, including (so far) a number of postings from e-mail lists that mac.com users have explicitly subscribed to. Worse, the messages are bounced back to the sender, but the recipient has no way of knowing anything is missing unless he or she is expecting something in particular. The only way the Mac user community found out about the filtering was when list administrators whose messages had been bounced contacted Apple to find out what was wrong.

The problem is particularly acute for those who use mac.com as their primary or only e-mail address, since there is rarely any way for

mistakenly blocked
"spammers" to contact them to let them know anything's wrong.
Users have no
way of knowing how much mail they may have missed.

The approach is also puzzling, since spam protection is usually
a benefit
ISPs and e-mail providers like to promote to their users. And in
most
instances they provide the option to deactivate or adjust it too.

Derek K. Miller - dkmiller@pobox.com, Writer, Editor, Web Guy,
Drummer, Dad
Vancouver, BC, Canada | <http://www.penmachine.com>

🔥 Apple: break your new PC with a copy-protected CD, it's not our fault

"Charles Arthur, The Independent" <carthur@independent.co.uk>
Fri, 10 May 2002 15:44:02 +0100

[From Dave Farber's IP,
<http://www.interesting-people.org/archives/interesting-people/>]

An interesting little endnote in
<http://kbase.info.apple.com/cgi-bin/WebObjects/kbase.woa/wa/query?searchMode=Expert&type=id&val=KC.106882>

(Apple tech note 106882)
which is mostly about how to get out one of those copy-protected
CDs, e.g.,
Shakira's "Laundry Service" if you put it in your Mac and the
thing goes
gray screen on you.

Lots of stuff about poke this and prod that. And at the end, a
note which I
translate to mean "Hey, nothing to do with us, you did the

equivalent of
sticking a fork in the toaster":

"CD audio discs that incorporate copyright protection technologies do not adhere to published Compact Disc standards. Apple designs its CD drives to support media that conforms to such standards. Apple computers are not designed to support copyright protected media that do not conform to such standards. Therefore, any attempt to use non standard discs with Apple CD drives will be considered a misapplication of the product. Under the terms of Apple's One-Year Limited Warranty, AppleCare Protection Plan, or other AppleCare agreement any misapplication of the product is excluded from Apple's repair coverage. Because the Apple product is functioning correctly according to its design specifications, any fee assessed by an Apple Authorized Service Provider or Apple for repair service will not be Apple's responsibility."

Interesting. So whose fault is it? The user's, one must surmise. But I foresee some more sticky labels - perhaps ADMIN ADVISORY - INCLUDES EXPLICIT WARRANTY BREAKING DATA

✶ Shipping the Big Iron: a computer-related risk!

Mike Hogsett <hogsett@csl.sri.com>
Fri, 10 May 2002 15:04:17 -0700

We recently arranged with Sun for them to lend us one of their

larger systems, a Sun Fire 4800. The machine has 208Gbytes RAM & 12 CPUs. Not a cheap machine. It is mounted within its own 72" tall cabinet. It is shipped in a wood crate which is approximately 3' wide by 4' deep by 8' tall. Gross weight is about 900 pounds.

Since their warehouse is just across the San Francisco Bay from us, they contracted with a local carrier to ship it to us. The machine was picked up from their warehouse, placed into the truck, and arrived at our receiving department a few hours later.

When the driver and our receiving personnel opened the trailer door, the crate was lying on its side, although it had been upright when it left the warehouse. The driver stated that he had heard a loud bang after making a turn and had thought he may have blown a tire.

On the crate there were several shock sensors and tilt sensors, only one of which had tripped (the one which was face up when it was on its side). There were also instructions telling us what to do if these sensors had been tripped.

The instructions told us to accept shipment but to inspect for damage and call the carrier. We did accept shipment but did not open the crate to inspect for damage. We contacted our representative at Sun for advice.

Our representative is having a replacement shipped to us and the unit which is here now will be picked up and sent back.

I was quite surprised that the crate was not strapped in and tied down tight given how narrow, tall, and heavy this crate was, not to mention the value of its contents.

Michael Hogsett

UK govt wants to make "e-filing" compulsory for taxes

David Cantrell <david@cantrell.org.uk>

Fri, 10 May 2002 18:38:14 +0100

This is taken from **Metro**, a [...] free tabloid distributed on trains and tubes in the London area. The same story appears in **The Register** and elsewhere:

E-mail taxman or face UKP3,000 fine, by Sarah Getty

Companies and individuals will be fined up to UKP3000 if they fail to file

tax figures via the Internet, it emerged yesterday. Measures proposed in

the government's new Finance Bill mean that so-called 'e-filing' of

payroll information will be phased in for larger businesses in the next

few years.

By 2010, all employers will be required to submit tax forms online.

But accountants fear elderly and disabled people who employ carers, or

people who use nannies, will be caught up in the legislation if they pay

through a payroll system. ... He also objected to the way

the Bill is

framed, which means little parliamentary scrutiny will be required is the

Inland Revenue or Treasury wants to extend the powers of the Bill...

The RISKS are obvious, both in terms of accessibility of this online filing system, but also the growing trend for legislation by regulation, thus allowing ministers to bypass parliament.

David Cantrell <http://www.cantrell.org.uk/david>

Verisign doesn't encrypt credit-card info

Daniel Norton <Daniel@DanielNorton.net>

Thu, 09 May 2002 07:45:16 -0400

Their slogan is "The Value of Trust", but why trust an organization that doesn't protect credit-card data when you sign up for a "Code Signing Digital ID?"

The actual URL is too long for inclusion here, but it's the link at the end of this page that reads "Code Signing Digital ID for Microsoft Authenticode" (above where it reads "US \$400.00 annually"):

http://digitalid.verisign.com/developer/ms_pick.htm

Fill out the form and include your credit-card number below where it reads "All enrollment and credit-card information is transmitted securely using the Secure Sockets Layer (SSL) protocol and VeriSign Server

IDs." But also
note the absence of any "secure" indicator on your web browser.

Press "Accept" and all form data is submitted in plain text to Verisign.

::slaps forehead::

The RISKS lesson? Don't trust anyone just because they say
"Trust me."

✶ Making a list, checking it never

Adam Shostack <adam@zeroknowledge.com>

Fri, 10 May 2002 11:48:31 -0400

Risks of mis-identification, arrest, etc, from law enforcement databases are well documented. The new, secret terrorism databases are starting to repeat these mistakes, as documented in a New Yorker article on a 70 year old black woman (Johnnie Thomas) is in a set of FBI databases, because "John Thomas Christopher" was an alias used by Christian Michael Longo, once on the FBI top ten most wanted list. Unfortunately for Johnnie Thomas, even the fact that Mr. Longo is in jail in Oregon hasn't removed her name from the computers, and the New Yorker article documents her (so far unsuccessful) attempts to clear her name.

http://www.newyorker.com/talk/content/?020513ta_talk_mcnamer

The application of fair information practices; allowing people to know what data is stored about them, to access and correct records,

etc, is often brushed aside for law enforcement claims that the data must remain secret. Does anyone know if these databases are the the Expanded Computer Assisted Passenger Screening Program, or something else?

✶ Re: The Console Buffer Knows... (Bergman, [RISKS-22.06](#))

Dick Mills <dmills@mybizz.net>

Thu, 9 May 2002 16:14:29 -0400

> However, I think that there's a RISK when someone uses an apparently
> "dumb" device with no intrinsic "history" to connect to another device
> (the switch) with no command history, and yet there's a record of every
> screen preserved weeks later.

True; but when we examine the totality of the risks archives, and Mr.

Neumann's book it becomes clear that the number of security pitfalls in computer use are so great in number, that even the most experienced and vigilant among us can't avoid making fools of ourselves fairly often.

My conclusion is that meaningful security comes only with the military approach of physically limiting access to computers and networks of computers containing secure information. Everything short of that has to be considered half measures and evidence that the information owner isn't really serious about security.

For the vast majority of the computing community that is not willing to take measures as extreme as the military does, the implication is that we must design our systems and procedures and set our expectations on the presumption that our work is not secure and can never be secure. At least in my humble opinion.

✶ Re: GNU is not UNIX (Maziuk, [RISKS-22.06](#))

"Theodore Ts'o" <tytso@mit.edu>
Thu, 9 May 2002 12:22:59 -0400

Dimitri's rant contains a number of inaccuracies as well as misconceptions or myths. [It also had a typo in the subject line that has been fixed in the archives for search purposes. It also provoked a lot of responses, some of which are interspersed by me within Ted's comments here. PGN]

First of all, with regards to Stallman's rants about "LiGNUx", this is a very long and often debated point. To claim that it has a good technical reason is very much stretching the argument. At its base it is fundamentally a social/political question, and it's all about the FSF trying to take credit for a very popular OS movement. Stallman himself freely admits that the reason why he tried to rename the operating system was to try to draw Linux Users (many of whom are primarily pragmatists who use it because it's best for what they want to do, and not for any kind of political reason) into embracing his particular political agenda

with respect to Copyleft and the FSF's definition of "Free Software".

Dimitri claims that "Linux" has lots of GNU software in it, when in point of fact, even the most highly inflated figure claimed by the FSF is 28% of a typical Linux distribution, and for some distributions, (for example SuSE) the percentage of FSF code compared to other Open Source code is far, far less. There are of course many other arguments and counter-arguments --- including the FSF's contention that the XFree86 code should be counted as GNU software because the FSF would have included it in their vision of a GNU system --- never mind the fact that XFree86 wasn't written by the FSF and isn't even distributed under the GPL. ("Any code is GNU if I say it is!") However, the arguments start losing technical and logical and even rhetorical integrity quite quickly, and I won't waste the RISKS reader's time with any more of it.

(It also should be noted that while Dimitri claims that BSD is not GNU, *BSD systems also uses the GNU toolchain, and many other pieces of GNU software; so where's the clear technical distinction between when something is GNU and when something isn't?)

Secondly, with respect to Linux the killall command, it should be noted that first of all, contrary to Dimitri's assertion, IRIX's killall does allow the "killall -HUP inetd" construction; as does NetBSD, OpenBSD, and Linux. So to say that this is unique to Linux is quite incorrect. Furthermore, Irix,

Linux, and OpenBSD killall implementations are all independent, and do not derive from the same source; the authors of each of them consciously made the same design decision. "Killall" as a program which kills all process and which does not take an argument is actually a System V'ism; it was never in BSD 4.3 or Version 7 Unix. [Dik Winter and Anton Ertl noted that Irix killall also is able to accept a processname and thus behaves like Linux killall. Anton Ertl and Toby Cabot both noted that Linux's killall is not GNU, it is from Werner Almesberger's psmisc package (and that is specific to the Linux /proc filesystem). PGN]

> Back in 1975 professionals designed an OS called Unix. Being professionals,
> they realised the need for certain design principles. Such as splitting a
> task into a number of smaller subtasks and designing a separate tool to
> handle each subtask (that does one thing, and does it well)
[0].

[Kragen Sitaker noted that Unix began in 1969, not 1975. True. Ken Thompson was on our Bell Labs Multics team until 1969, and Oleg Broytman noted that Unix was designed *for* professionals (and primarily for their own use!). PGN]

This design principle is oft quoted, but rarely in its entirety. The *other* half of the Unix design principal was to observe what combinations of commands were frequently used, and optimize those. So for example, although you could search files looking for a particular pattern by using

/bin/ed's "g/<re>/p" command, it was used often enough that it was worth while for the Bell Labs "professionals" to create the command "grep".

If only the first part of the Unix minimalist design principle was all there was to it, there would be no need for the grep command. Heck, there would be no need for the System V "killall" command --- it would be possible to implement it via smaller sub-components, so by what rights should it exist? Indeed, the System V "killall" command is used so rarely (only by the shutdown scripts), that arguably, it shouldn't exist at all, even using the argument which justifies the existence of grep. It's only used in one instance, so there's no justification for optimizing it or packaging it as a stand-alone command.

In addition, the reason why people get into trouble when trying to run "killall -HUP inetd" on a Solaris machine is because the Solaris version doesn't check the arguments it was passed; a well designed and robust program should check the validity of its arguments, and fail if they are not what was expected --- and this includes the presence of arguments when none are supported.

For this reason, since the System V killall is such a useless, unjustifiable, badly implemented botch of an idea --- let me defend the honor of the "1975 professionals" which Dimitri invoked by stating that killall was not their fault. It was the fault of the people at AT&T who among other things, gave us abominations such as System V

streams. [To
amplify that, Peter van Hooft notes that there was no killall in
Version 7,
and Anton Ertl did similarly. PGN]

So to the extent that the Linux, *BSD, and Irix maintainers all
decided to
ignore this "prior art" in favor of something much more useful,
this was a
Good Thing. After all, "killall -HUP inetd" is far more useful
and commonly
used that it's worth being able to do this rather forcing the
system
administrator to type:

```
kill -HUP `ps ax | grep inetd | awk '{print $1}'`
```

Don't you think?

> As software becomes more complex, it requires more
sophisticated build
> tools. More and more open source software is being developed
using GNU
> compilers and build tools, and it is becoming dependent on
them. The result?
> -- While portability at the level of each compilation unit is
still
> maintained, the whole thing is not portable anymore. It fails
to build on
> non-GNU systems [2].

This is an old problem, and it's not unique to GNU or Linux ---
remember
back in the days of BSD 4.3, and Henry Spencer's 10th
Commandment of his
"Ten Commandments of Unix"?

"10. Thou shalt forswear, renounce, and abjure the vile
heresy which
claimeth that ``All the world's a VAX'', and have no commerce
with the
benighted heathens who cling to this barbarous belief, that
the days of

thy program may be long even though the days of thy current machine be short."

The annotated version <http://www.lysator.liu.se/c/ten-commandments.html>

points out that an updated version of this heresy would be "All the world's a Sun". In the years before Linux became ascendent, I remember having to work with lots of programs available on the Internet which only worked on Solaris machines, and didn't compile or run correctly on Ultrix or OSF/1 machines. This is not a new issue; your claim that this is somehow unique to GNU/Linux systems is simply not fair nor historically accurate.

The main problem is that most of the bug-fixing takes place on those platforms which are most easily available no matter what it was. Back in the day when the development community had plenty of VAX systems running BSD 4.3, guess what most programs were optimized for? And back when most people with Internet access were running SunOS, guess what most programs were most likely to run under?

Sun is actually partially at fault here, actually, at least with respect to the problem you stated of many programs assuming the use of the GCC and the GNU toolchain. Back when Sun stupidly started charging for their C compiler as a separate, optional package, and never looked back, many people switched to using the GNU toolchain, and never looked back. Given that GCC is available for Solaris, the incentive to making packages portable to the

native tool chain is simply much, much less. (But hey, if it's so important to you, the whole point of Open Source software is that you can fix the problem yourself, and contribute the changes back to the maintainer.)

>And since GNU compiler and build tools are unable to produce 64-bit code on Solaris, the libraries, and all software that uses them must be built as 32-bit binaries. Now, why did I pay for that 64-bit hardware, again?

Actually, that last is a very good question. Unless you needed the address space the 64-bit provides, in most cases there is no advantage to compiling programs to run in 64-bit mode. Indeed, to the extent that the pointers and integers take up more space, programs can actually run more slowly and take up more memory unnecessarily when you compile them as 64-bit binaries. Given that most of the Open Source programs you want to run probably don't need the 64-bit address space (very few programs, other than scientific computation and database engines do), the fact that you're compiling GNOME or Gnumeric in 32-bit mode is probably the right thing; it's certainly not a problem. [Anthony W. Youngman notes that linux ran on SPARC in full 64-bit mode long before Solaris did. PGN]

> GNU project in particular did a great service to software community by promoting and popularizing free software. It also did a great disservice by turning the whole thing into a political issue, and pretty much ignoring the need for competence and expertise on the part of software

developers.

> Instead of sound software engineering, we now have "Free Speech"

> flag-waving [3].

First of all, many members of the Linux development community don't pay much attention to the FSF's political agenda. (This is the whole reason for the "Open Source" vs. "Free Software" terminological debate, which in turn inspired Stallman to try to claim Linux as his own by trying to rename it to LiGNUx"; as I said, this is not a technical issue, but a political one --- and many, many people in the Linux world do not subscribe to the FSF political agenda.)

Secondly, it's very much unfair to make such a huge generalization; many open source software packages are written or maintained by professionals, and it shows. Some of it isn't. In general, software which works gets used. Software which doesn't, doesn't get used. People don't choose to use Linux because of the FSF's political agenda; they use Linux (or FreeBSD, or MacOSX) because it does what they need it to do; because it crashes less often than Windows; because they are able to "look under the hood" and fix themselves if necessary, instead of being at the mercy of vendor who might or might not deign to fix a bug which is critically affecting your business.

Open Source software may not be perfect, but then again, no commercially available operating system which is available at reasonable prices is perfect, or even close to perfect. The stories in RISKS have

proven this
over and over again.

[RISKS received numerous counter-rants (NOTE: ``counterrants'' might seem like count-errants, as in knight-errants), including admonitions to your moderator for running Dimitri's rant in the first place. But the mere existence of his rant suggests that some education is needed, and hopefully Ted's message has provided some. I have interspersed a few of the comments received as they apply above. PGN]

✶ Re: GNU is not UNIX (T'so, [RISKS-22.07](#))

Dimitri Maziuk <dmaziuk@yola.bmrb.wisc.edu>
Thu, 9 May 2002 13:06:18 -0500

[Dimitri's own counter-counter-rant is excerpted here by PGN.]

Most software licenses that I bothered to read expressly disclaim "any warranty as to suitability or fitness for any purpose". To me, that spells "crap".

Commercial developers are at least [implicitly] honest: they're here to make money. If they can make money from crap, more power to them.

When crap is being pushed as the best thing since sliced bread because it's "Free as in Beer" (or "Speech", or whatever) (read: "it makes some nerd with zero social skills feel good about himself"), well, forgive me if all I feel

about that is disdain.

I'm a great believer in Open Source, Public Science, and sharing of ideas. But you know what? -- my job is to keep software up and running. I don't care if it pays someone's bills, or if it suits someone's political agenda. All I care about is that it works.

And in my experience software that works is software written by clueful developers -- professionals, experts, -- be that Wietse Venema, Linus Torvalds, or Borland language design team.

None of which has anything to with the fact that GNU is Not Unix, and as more people come to grown-up Unices from GNU background, screw-ups like the one with killall will become more and more common.

PS. As for 64-bit hardware, here's a hint: if you have SPARC Solaris 7 or 8, run this script:

```
#!/bin/bash
if [  $\$(2048*1024*1024)$  -lt 0 ] ; then echo "Your bash has Alzheimer's" ; fi
```

and see what it says. And if you have any shell scripts that e.g. monitor RAM or disk usage, better go check them really carefully.

🔥 More on Klez (Re: Slade, [RISKS-22.05](#))

"Bob Morrell" <bmorrell@wfubmc.edu>

Thu, 9 May 2002 12:18:12 -0400

Rob Slade's comments on Klez was a useful summary of the broader aspects of this recent worm.

I agree that the unusual lack of publicity on this worm is puzzling and problematic. However, the much more disruptive aspect of this worm which Mr. Slade mentioned has been Klez's penchant for sending e-mail in other people's name.

Person A, gets the virus, and his computer sends an infected e-mail to person B in the name of person C. At this point several things can happen, all of which cost the users (and their Network admins oodles of time).

The most common is that person B sends an angry e-mail to person C (whom they often do not know) or worse, to person C's business/domain. Non computer system admins want to know what person C is doing (and their questions are more pointed when Klez uses a sexually suggestive subject header). They look suspiciously at C, and at C's LAN admin, who had certified that C's computer was patched and had adequate virus protection. Explaining the complexities of this worm to less than computer literate admins often takes two or three attempts, and even then I think some of them still think they should ding someone.

Person B has a server based e-mail viral scanner and sends a notification of failure to deliver to C, who flips out, believing their computer is infected. Again, the complexities of this worm are hard to communicate, and much time is wasted trying to explain, and all the assurances you have given them about how up to date and secure their computer is (and why it is worth

all the time and effort you put into antiviral and patches) suffer a credibility hit. User C may even try to contact B's domain seeking an explanation (and more time is wasted on all sides).

This is in effect, a new form of identity theft, and the time wasted in orientation (what is going on?) and repairing perceptions and reputations can be substantial.

The risk? Too many e-mail users still believe that 'from' header, unaware how easy it is to fake. As Klez forces them to understand this, they almost certainly will over-react, which ultimately will undermine the efforts to make digital signatures and online validation more common.

Bob Morrell, Cancer Center, <http://home.triad.rr.com/bmorrell/>

⚡ Re: More on Klez (Re: Slade, [RISKS-22.05](#))

Bitwolf Programming <mp0283@bitwolf.net>

Thu, 09 May 2002 01:47:17 -0400

I have a minor addition to Rob Slade's observations and comments. Though not vulnerable myself to Klez, I've had to deal with infections on a number of e-mail lists. To my experience, the Return-Path header generally contains the infected person's address, or enough of a clue that you can narrow down the listmember[0] who might be infected. Given that this is malware, there is a RISK in relying on it, but for the moment it

does
provide clues useful in identifying and alerting folks with
infected
machines.

Paul Mech

[0] Many folks on an e-mail list will have other people from the
list
bookmarked. Thus some of the malware's forgeries will fool some
lists into
accepting it's spawn.



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

[ACM](#) Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 8

Wednesday 22 May 2002

Contents

- [SPAM-demon-ium overload countermeasure](#)
[PGN](#)
- [AT&T's e-mail filter filters AT&T's e-mail](#)
[NewsScan](#)
- [Air-traffic control software reliability](#)
[Peter B. Ladkin](#)
- [Disk crash destroys law-enforcement mug shots in Michigan](#)
[Thomas Insel](#)
- [WashDC database crash linked to a death by a falling tree](#)
[Przemek Klosowski](#)
- [Fun with fingerprint readers](#)
[Bruce Schneier via Monty Solomon](#)
- ["Medication errors could be eliminated ..."](#)
[Dr. David Alan Gilbert](#)
- [Copy Protected CDs -- risk of selling marker pens](#)
[Doug Sojourner](#)
- [Re: Apple: break your new PC with a copy-protected CD ...](#)
[Bill Bumgarner](#)
- [FBI does not care about standards, nor getting that information](#)
[Peter Ha*kanson](#)

- [2 unsolved telephone mysteries - software faults?](#)
[Andrew Goodman-Jones](#)
 - [Candy machine punishes the quick-thinking](#)
[Fredric L. Rice](#)
 - [Compaq issues refunds for one-cent PCs](#)
[Tudor Bosman](#)
 - [Re: Your bash has Alzheimer's](#)
[Bob Bramwell](#)
 - [REVIEW: "CISSP Exam Cram", Mandy Andress](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ SPAM-demon-ium overload countermeasure

RISKS List Owner <risiko@csl.sri.com>

Weds, 22 May 2002 10:12:43 PDT

I was away from the RISKS directory for almost a week, and went an overly long 10 days between [RISKS-22.06](#) and [22.07](#). Out of over 1000 e-mail messages in a 6-day period, there were about 20 potential contributions, and one message from a would-be subscriber whose mailer had mistakenly sent his "accept" response to RISKS rather than replying to majordomo. About *98 percent* of the RISKS e-mail during that period was spam that I deleted unseen based only on the subject message or the From: address. (Excuse me if I accidentally deleted one of your legitimate submissions!) The RISKS spam rate has enormously increased over the past year (when I mentioned it in [RISKS-21.39](#), one year ago, it had just reached 50% for the first time).

At 98%, it has now reached absolutely ridiculous proportions and necessitates some draconian action. For example, we could use some sort of challenge-response confirmation technique and hope that your mail systems will be able to cope with it; however, as we have read here in the past, such schemes can create further risks. CONSEQUENTLY, as a simpler measure, we have just installed SpamAssassin (free software from spamassassin.org), and in the first few minutes it is **already** a huge success as the spam pours into another mailbox that I hopefully will seldom look at. Of course, SpamAssassin may also filter out some of your legitimate mail, without letting you know. So, if you have sent in an absolutely marvelous contribution or an urgent request and believe that I may never have seen it, please send an out-of-band message to that effect.

Incidentally, the annual seasonal RISKS slowdown will begin as usual this year in mid-June, which means just a few issues now and then over the northern hemisphere's summer. Let's hope there are not too many disasters needing to be reported during that period.

Stay tuned. PGN

⚡ AT&T's e-mail filter filters AT&T's e-mail

"NewsScan" <newsscan@newsscan.com>

Wed, 22 May 2002 08:27:09 -0700

An example of foot-in-mouth filtering? AT&T Broadband offered

its high-speed
Internet users an e-mail software filter to block spam, but
later found out
that it had blocked its own messages to customers notifying them
of a rate
increase. An AT&T executive tried to put the best face on it:
"If there is a
silver lining, it appears our spam filtering system works so
well that it
even deletes mass e-mails from our own company." The company
will resend
customer notices of the rate increases. [AP/*USA Today* 2002;
NewsScan
Daily, 22 May 2002]
[http://www.usatoday.com/life/cyber/tech/2002/05/22/e-mail-
filter.htm](http://www.usatoday.com/life/cyber/tech/2002/05/22/e-mail-filter.htm)

✈ Air-traffic control software reliability

"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>
Wed, 15 May 2002 10:03:39 +0200

An article in **Aviation Week and Space Technology**, "Why
Controllers Are
Skeptics Regarding New Technology", by Bruce Nordwall, 6 May
2002, pp.50-51,
tells the following tale recounted recently at an air-traffic
controllers'
conference by Philippe Domogola, supervisor at the Maastricht
Upper Area
Control Center.

"Some years ago," a new European ATC center installed software
specified as
"99.99% reliable", which apparently meant 99.99% availability in
each
calendar year, or a maximum of roughly 52 minutes down-time per
year. The

software "failed" a couple of months after installation, and suffered 20 hours down-time. "The manufacturer's conclusion was: human error that will not happen again" (come to think of it, any specific software bug can be put down to "human error that will not happen again").

Someone had forgotten about leap years. It failed at 23:59 on February 28.

Some controllers suggested that since the software was "99.99% reliable" and it had failed for 20 hours, it follows there were going to be no more failures for the next 25 years.

They were right. It does follow.

Peter B. Ladkin, University of Bielefeld, Germany
<http://www.rvs.uni-bielefeld.de>

✶ Disk crash destroys law-enforcement mug shots in Michigan

Thomas Insel <tinsel@tinsel.org>
Sat, 11 May 2002 12:56:07 -0700 (PDT)

On 11 May 2002, *The New York Times* (page A13 of the National Edition) reported that the Macomb County, Michigan, sheriff's department lost over 50,000 photographs of criminals on a crashed hard drive. Not particularly exciting, except that they had wisely made hardcopy backups of some of the photos. The issue of electronic backups was never even raised. Perhaps many computer users no longer realize such a thing is possible?

<http://www.nytimes.com/2002/05/11/national/11BRFS.html>

🔥 WashDC database crash linked to a death by a falling tree

Przemek Klosowski <przemek@tux.org>

Sat, 18 May 2002 23:15:08 -0400

Among the world cities, the beautiful Washington DC is probably right up there in terms of a number of parks and wooded neighborhoods; it is possible to drive into the center of the city on roads that are visually completely surrounded by trees.

Unfortunately, the DC city government is still struggling with many municipal services; the city is sometimes few stray blocks short of Mary Poppins' proper child nursery. Tree maintenance is a particular problem: many trees have dead branches, and some are sick or dead. In the recent wave of violent spring storms, quite a number of trees were partly or completely felled, causing significant property damage, some injuries, and at least one death:

<http://www.washingtonpost.com/wp-dyn/articles/A17238-2002May14.html>

Part of the reason for this is the usual lack of funds and bureaucratic inertia, but there's also a computer angle:

"One major obstacle for the city is that its database of public trees that needed pruning or removal crashed in 2000 and

couldn't

be restored. At that time, the city had a backlog of 5,000 dead trees that needed to be removed. Now, it doesn't know how many it has."

⚡ Fun with fingerprint readers

Monty Solomon <monty@roscom.com>

Fri, 17 May 2002 17:27:36 -0400

Excerpted from Bruce Schneier's CRYPTO-GRAM, May 15, 2002

Tsutomu Matsumoto, a Japanese cryptographer, recently decided to look at biometric fingerprint devices that attempt to identify people based on their fingerprint. For years the companies selling these devices have claimed that they are very secure, and that it is almost impossible to fool them into accepting a fake finger as genuine. Matsumoto, along with his students at the Yokohama National University, showed that they can be reliably fooled with a little ingenuity and \$10 worth of household supplies. [...]

<http://www.counterpane.com/crypto-gram-0205.html#5>

[They were able to spoof 80% of the machines. PGN]

⚡ "Medication errors could be eliminated ..."

"Dr. David Alan Gilbert" <gilbertd@treblig.org>

Sun, 19 May 2002 19:52:48 +0100

The Pharmaceutical Journal (a journal for U.K. Pharmacists)
Vol 268, page
697, in an article on the sixth annual conference on electronic
prescribing
and medicines administration, has a picture of a health
professional using a
computer with the caption:

'Medication errors could be eliminated by the use of
electronic prescribing
systems'

The accompanying article (and another in the same issue) is more
careful to
say 'reduce' errors; but it is another example of the danger of
what a
computer can be expected to do.

Dr. David Alan Gilbert gro.gilbert @ treblig.org <http://www.treblig.org>

✶ Copy Protected CDs -- risk of selling marker pens

Doug Sojourner <doug_sojourner@agilent.com>
Mon, 20 May 2002 13:13:17 -0700

> ``Copy-Proof'' CDs Cracked with 99-Cent Marker Pen, 20 May
2002,
> By Bernhard Warner, European Internet Correspondent
> Technology buffs have cracked music publishing giant Sony
Music's
> elaborate disc copy-protection technology with a decidedly
low-tech
> method: scribbling around the rim of a disk with a felt-tip
marker.

Given that marking pens can be used to overcome Sony's CD

protection scheme,
will it now become illegal to sell pens?

★ Re: Apple: break your new PC with a copy-protected CD ... ([R 22 07](#))

Bill Bumgarner <bbum@codefab.com>

Sun, 19 May 2002 10:43:54 -0400

Is it a car company's fault if you put sugar water in the gas tank and it destroys the engine?

Is it a printer manufacturer's fault if you put toilet paper through your printer and completely destroy the print heads?

No -- is the consumer's fault in those cases.

In the case of the copy protected CDs, things aren't so clear. It still isn't the computer manufacturers fault-- at the time of design and manufacture, they cannot predict changes in technology and they certainly can't predict and account for changes in technology that are designed to break their products!

The problem with the copy protected audio CDs is that the CD manufacturer has purposefully designed a CD to be incompatible with computer hardware.

They have purposefully violated a standard that hardware manufacturers have been manufacturing to for nearly two decades (since 1983/1984).

Let's rephrase the question slightly:

Should it be legal for antitheft devices to destroy property?

In

particular, should it be legal to destroy property in contexts where it is

not 100% guaranteed that a theft was actually in progress?

That is exactly what the audio CD manufacturers (to be fair, the folks

mastering the CDs) are doing. They are purposefully creating a piece of

media that, when inserted into a computer, can cause data loss [a number of

PCs outright crash when faced with these CDs] or even changes to the

hardware that require relatively nasty fixes (as is the case with the Macs

-- it doesn't hurt it, just leaves it such that there is no way to get the

damned disk out).

Sure -- it may be the fault of the consumer for actually sticking the CD into

their computer.

But it would seem that the folks that created the format in direct violation

of published standards should share some of the blame and resulting

liability.

⚡ FBI does not care about standards, nor getting that information

peter h <peter@manet.nu>

Sun, 19 May 2002 11:22:58 +0200

A few days ago I noticed that one of my children got spam in his mailbox.

Browsing through it, it looked very nasty, advertizing child-

pornography. As this is a crime both in my country and in Maryland, USA, I decided to report it.

Finding www.fbi.gov was easy. Finding an e-mail address was difficult. In fact, I failed finding an e-mail address. What was available was one of those Webforms that never really is appropriate for the task in hand. As the Webform was the only alternative, I tried to register my complaints, hoping that someone would contact me via e-mail so all details could be reported.

Within hours there was an attempt, I say attempt because my mailserver is configured to reject connections from abusive and rfc-ignorant sites. A common technique that spammers hide behind is sending e-mail from a domain that does not exist. Those mails can never be replied to, nor complained about.

Guess what? the connection attempt was from <NO-Reply-IFCC@zorin.ifccfbi.gov>

I see two problems with FBI'S attitude. The serious one is that they will miss some tips and e-mails with data (not everyone has an explorer browser available). The other problem is that their IT-responsibility seems to be totally clueless.

What's most important? To get those tips - or to make sure that everyone uses Microsoft Explorer whenever they contact FBI. I have my opinion, but unfortunately I cannot vote in the US.

I also sent a copy of the same mail to the Swedish police, where I could find e-mail addresses, but they seem to have ignored the report.

2 unsolved telephone mysteries - software faults?

"Andrew Goodman-Jones" <goodie@ozemail.com.au>

Thu, 23 May 2002 00:48:22 +1000

It's 5am. My mum gets woken by one ring on her home phone. It stops before she can answer it.

Being her curious and paranoid self (wonder where she gets that from?), she gets up anyway and checks the Caller ID unit. The number is her own mobile. Her mobile is in her bedroom on the table. It has a flip down panel that covers the keypad (which prevents accidental dialing by bumping the buttons). She checks the recent outgoing calls list (after asking me how to view it). Her home number is in the list.

How did her mobile phone make a call by itself at 5am?

It is believed that no-one else intervened in this situation (i.e., cat-burglars, children etc)

Anyone have any ideas? (BTW, it's a Samsung GSM phone if that helps. I have the same model and this has never happened to me, that I know of.)

This is the second on my list of Weird Stuff. First on the list is:

Back in 1996 when I went to NYC, a call was made from my phone in my office in Sydney a few days after I had left. Ok, not too weird - it was probably the other guy I was sharing the office with. Here's the weird bit: A call at a very similar time was made on my HOME phone to the same number (which I don't recognise at all). No-one from the office had any association at all with my home. Different bills, different suburbs, different exchanges etc. I have no idea at all what happened here.

I reckon that both events were software faults. The first in the mobile phone's firmware, the second at the billing dept. of the phone company.

Andrew Goodman-Jones <goodie@ozemail.com.au>

✶ Candy machine punishes the quick-thinking

"Fredric L. Rice" <frice@SkepticTank.ORG>

Thu, 09 May 2002 13:12:03

While picking up my company snail mail, I observed a guy shove a dollar bill into a candy vending machine, slowly look over the selections, and then punch in a choice. He was rewarded with not only candy but also change for his buck. Good deal; everybody walked away happy.

There were some mints in the machine that I wanted so I walked up, shove my dollar into the machine, and punched D2 only to be rewarded with

an "ERROR:
Cost \$.70" message and no sign of my dollar. After a minute or
two of
pounding, kicking, and yelling at the machine (I'm a programmer)
I tried
again (I'm also a sucker) only this time I shoved in the dollar
and waited
for the display to show "Credit: \$1.00." When I made my
selection -- D2
again -- this time I got my mints and my change.

It turns out that there's a period of time between when you
shove in your
buck and get the "Credit: \$1.00" message that if you make a
selection the
machine will eat the dollar and then swear up and down you never
gave it
one.

Funny, though, that people who know exactly what they want in
life before
they pay their money are the ones who get rooked the most while
the people
who shove in their buck and then examine the variety of
available choices
life has to offer are the ones who get rooked less.

The risks? I suspect that the software that went in to the
machine was
tested by the programmer and not tested in the field before
being released
-- though the only way to find out would be to ask. Not doing
real-world
testing is a common risk but this fault was dumb and should have
been easy
to catch before the software was released.

[Just wait until the thing starts accepting debit and credit
cards. More

good ways to make the software fail! }:-}]

[So, we need atomic transactions from a candy machine! PGN]

✂ **Compaq issues refunds for one-cent PCs**

Tudor Bosman <tudorb@Stanford.EDU>

Sat, 11 May 2002 12:16:49 -0700

The RISK is obvious. From <http://zdnet.com.com/2100-1106-903686.html>:

Despite its initial denials, Compaq Australia now admits that it did in fact process the payments of customers who bought Presario laptops for just one cent as a result of an online pricing hiccup. [...] Compaq is still adamant, however, that it is not obligated to honor the accidental one-cent pricing, despite mounting industry criticism and ongoing threats of a customer-initiated class action law suit. [...] "As this was a genuine error, Compaq canceled all orders from the system. In instances where 1 cent was debited from customers accounts it will be refunded."

✂ **Re: Your bash has Alzheimer's (Maziuk, [RISKS-22.07](#))**

Bob Bramwell <bbramwel@shaw.ca>

Sun, 19 May 2002 03:28:08 +0000 (GMT)

Interestingly enough, not merely is my bash mentally deficient, but so is ksh, sh, csh, and tcsh. This is on a SunBlade 100 running Solaris 8. Now, what does this say about Korn, Bourne, Joy, and Grevstad I wonder? Methinks

it is a little unfair to single out Larry Wall for such criticism, but I appreciate the "heads up"!

Bob Bramwell, ProntoLogical, 60 Baker Cr. NW, Calgary, AB T2L 1R4, Canada
+1 403/861-8827

★ **REVIEW: "CISSP Exam Cram", Mandy Andress**

Rob Slade <rslade@sprint.ca>
Mon, 13 May 2002 11:56:34 -0800

BKCISPEC.RVW 20020321

"CISSP (Exam Cram)", Mandy Andress, 2001, 1-58880-029-6,
U\$34.99/C\$53.99/UK#24.49

%A Mandy Andress
%C 14455 N. Hayden Road, Suite 220, Scottsdale, AZ 85260
%D 2001
%G 1-58880-029-6
%I Coriolis
%O U\$34.99/C\$53.99/UK#24.49 800-410-0192 fax: 602-483-0193
%P 265 p.
%T "CISSP (Exam Cram)"

It is interesting, and somewhat disturbing, to note that while there are a number of effusive quotes on and inside the cover extolling the virtues of the Exam Cram series, none specifically mention this book.

Bound into the inside front cover is a cram sheet, with 50 points on

it that are obviously supposed to be vitally important to the exam.

Leaving aside both the simplistic nature of the information presented,

and the difficulty of answering a 250 question exam with a mere

50

points, we only have to get to the third point on the sheet before we run into rather significant errors. (Role-based access control is not an alternative to discretionary or mandatory controls, but can implement either.) This does not bode well.

The introduction explains the CISSP (Certified Information Systems Security Professional) designation. The text makes frequent references to the (ISC)² web site, but, since the recent site redesign, all these URLs are incorrect. There is also a short self-assessment section, intended to help you determine whether or not you are prepared for the exam, but the vague and generic metrics suggested are unlikely to help determine your readiness.

Chapter one's discussion of the exam, and techniques for writing the exam, does contain some useful recommendations (if you don't know, answer anyway), but other advice is problematic, and may be detrimental. Access control, in chapter two, is the first of the ten domains of the Common Body of Knowledge (CBK) of the CISSP. The material is presented as a list of key terms and phrases, and the presentation might be helpful to the exam candidate were it not for the extremely limited nature of the deliberation and frequent errors. For some reason a significant amount of space is given to topics (like SYN floods) that do not belong in this domain. There is a brief list of questions at the end of the chapter, with answers and discussion presented immediately afterward. Unfortunately, these questions are so

simplistic that they cannot be said to represent, in any way, the exam itself, and the wording is so careless that it is often impossible to say whether the answers given are, in fact, right or wrong.

Chapter three provides an almost random assortment of topics related to telecommunications and networking. (There is a modicum of structure in that subjects are grouped together, but there is no logical flow: IPsec is discussed before the base IP concepts are covered.) There are many problems with the material: it is difficult to say whether the definition of a "circuit gateway" firewall means anything, let alone is right or wrong, and we are told that SSL (Secure Sockets Layer) is only used for host-to-host communications and resides in the session layer. (The book contradicts itself: chapter six does note that SSL is used between client browser and web server.) Again, many irrelevant topics are included while important areas are missed. (PPP (Point-to-Point Protocol) is listed, PPTP (Point-to-Point Tunnelling Protocol) is not.) Security management practices are not covered in chapter four: the vital areas of policies and risk analysis are given brief mention at the end of a meandering and incomplete list of management concerns. Another haphazard catalog of terms takes the place of the applications development domain in chapter five. (The definition of a virus is that of a trojan and the definition for a worm seems to fit payload.) That the author is unfamiliar with basic concepts of cryptography is obvious when, in chapter six, "strong encryption" is defined

as the use of a 128-bit key. (In the discussion of triple DES (Data Encryption Standard), the "meet-in-the-middle" attack is obviously confused with "man-in-the-middle.") Chapter seven's review of security architectures contains another arbitrary list of computer architecture topics. There is some material that is security related, but in the discussion of the Bell-La Padula model, about the only reliable information is that it involves security levels. Operations security is fairly straightforward, so chapter eight doesn't make any glaring errors. (The content is, however, very terse.) Much the same holds true for business continuity and disaster recovery in chapter nine. Aside from an over-emphasis on US legislation, chapter ten does not do a really bad job with law, investigation, and ethics. Chapter eleven collates some checklists related to physical security, but has numerous gaps in the discussion of the overall topic.

About the best that can be said for this book is that most of the items in the common body of knowledge get a mention at some point. Beyond that, the material is too scattered and unreliable to be used either to study for the CISSP exam (unless you want to play "spot the error"), or even as a quick guide for those charged with security.

copyright Robert M. Slade, 2002 BKCISPEC.RVW 20020321
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

<http://victoria.tc.ca/techrev/~rslade> or <http://sun.soci.niu.edu/~rslade>

[Perhaps Coriolis can Force you to pass the exam? Quite a spin! PGN]

✶ 11th USENIX Security Symposium (excerpted for RISKS)

Alex Walker <alex@usenix.org>

Mon, 20 May 2002 10:43:19 -0700

11th USENIX Security Symposium
August 5-9, 2002, San Francisco, California
<http://www.usenix.org/sec02>

Register online by July 10, 2002, and SAVE up to \$400!

KEYNOTE SPEAKER, Whitfield Diffie, Distinguished Engineer, Sun
Microsystems speaking about "Information Security in the 21st
Century"

Simon D. Byers, ATT Labs - Research

Professor Edward W. Felten, Princeton University.

Paul Kocher, Cryptography Research, Inc.



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 9

Thursday 23 May 2002

Contents

- [Re: S-P-A-M-demonium](#)
[PGN](#)
[Kevin](#)
- [Computer failure grounds over 300 flights in minutes](#)
[Chris Brady](#)
- [Air-traffic controllers can't read the new screens](#)
[Chris Brady](#)
- [Paper: How to own the Internet in your spare time](#)
[Nicholas C. Weaver](#)
- [Credit-card data from wireless registers](#)
[Jim Laurenson](#)
- [Ford Motor Credit office baffled by theft](#)
[Dave Hansen](#)
- [Vending Machines - Poor Programming](#)
[T.J. Griesenbrock](#)
- [RISKS of providing smart-alecky false information](#)
[Daniel P. B. Smith](#)
- [Phony 'soldier' needs your help giving him your money](#)
[NewsScan](#)
- [Re: Fun with fingerprint readers](#)

[Arnt Gulbrandsen](#)

● [Re: 2 unsolved telephone mysteries](#)

[Stanislav Meduna](#)

[Chris Barnabo](#)

● [Re: Copy-Protected CDs](#)

[Jan Ingvoldstad](#)

[Sean A Dunn](#)

[Russ Perry Jr](#)

[Martin Ward](#)

● [Re: More on Klez](#)

[Joseph Brennan](#)

● [REVIEW: "Cyber Forensics", Albert J. Marcella/Robert S. Greenfield](#)

[Rob Slade](#)

● [Info on RISKS \(comp.risks\)](#)

✶ [Re: S-P-A-M-demonium \(RISKS-22.08\)](#)

"Peter G. Neumann" <neumann@csl.sri.com>

Wed, 22 May 2002 13:18:00 PDT

My lead message in [RISKS-22.08](#) announcing the use of a filter resulted in those of us using that filter to have the issue designated as s-p-a-m! If you did not receive that issue because YOUR filtering is configured to pipe the message off to somewhere else or to delete it altogether, then you may pick [RISKS-22.08](#) up at [www.risks.org](#). But the effect of installing that filter was very dramatic, having taking the RISKS spam rate instantly from 98% to close to 0%.

The false positive trigger on [RISKS-22.08](#) resulted largely from one triggers:

Hit! (4.4 points) BODY: O-n-e h-u-n-d-r-e-d p-e-r-c-e-n-t g-u-a-r-a-n-t-e-e-d

which had to do not with s*p*a*m, but with fraud detection.

[Hyphens inserted to minimize further false positives? PGN]

Incidentally, because of the new regime, I will be able to look at more messages from you all, in the same amount of my limited screen time.

⚡ Re: S-P-A-M-demonium ([RISKS-22.08](#))

Kevin <nobody@tex.kom>

Thu, 23 May 2002 17:24:19 GMT

Also install Vipul's Razor if you can, from razor.sourceforge.net .

My own experience is that SpamAssassin is the best spam trapper I've ever

used, and I've tried a lot of them over the last several years.

But, make

sure you have auto-whitelisting turned on. You also might want to salt your

config file(s) with whitelist and blacklist information based on your

history, which SpamAssassin won't know about yet. Once I did that salting,

my false negatives and false positives dropped to zero per month, but I only

process 10Meg of mail in that time.

⚡ Computer failure grounds over 300 flights in minutes

Chris Brady <chrisjbrady@yahoo.com>

Thu, 23 May 2002 12:29:19 +0100 (BST)

Yet again the new multi-million-pound air-traffic computer system at Swanwick near Heathrow crashed last Friday (May 17, 2002) shortly after 6.30 am.

This is a time of maximum inbound flights from the Middle and Far East -- with full 747's arriving at one a minute. Also too it is just when the morning rush hour for domestic and European departures and arrivals begins to build up.

The crash was the result of a 'routine upgrade' which made half the air traffic controllers' computer screens inoperable. This meant that only half the normal flights could be handled. This meant that airlines had to cancel most of their flights into and out of Heathrow - a situation which lasted for most of the day. Imagine one flight being canceled and all the disruption that can cause, then multiply that by many hundreds. And the knock on effect of the wrong planes and crews in the wrong places at the wrong times lasted for most of the following weekend. The consequent loss of revenue to the struggling airline industry is inestimable, to say nothing of the increased loss of confidence in the safety of flying amongst the traveling public.

The risks are obvious. The new computer system at Swanwick is a disaster waiting to happen. A 'routine upgrade' should not result in a major loss of service. The upgrade was obviously made to the primary system

before
testing on any back up system (is there one?), and if a routine
upgrade can
cause such a system loss then what would happen to a major
upgrade?

Confidence in the safety of the ATC system at Heathrow is not
increased with
the U.K. Government's refusal to financially bale out - yet
again - to the
tune of millions of pounds - the owners of the new system, the
privatised
NATS (National Air Traffic Services).

✈ Air-traffic controllers can't read the new screens

Chris Brady <chrisjbrady@yahoo.com>
Thu, 23 May 2002 12:10:41 +0100 (BST)

Confusing screens at Swanwick's new air-traffic control centre
near Heathrow
have resulted in aircraft being directed towards the wrong
airports.
Controllers have also misread the altitude of aircraft because
letters and
numbers are difficult to distinguish on the screens, according
to the **Daily
Mail**, 23 May 2002. For example, the numbers 0, 8 and 6 are
confused,
leading to mistakes of thousands of feet in the height of
flightpaths
(noted in a report in **Computer Weekly** magazine).

Controllers and their supervisors at the privatised NATS
(National Air
Traffic Services) centre at Swanwick have detailed the errors in
a health
and safety report, which revealed that one controller has
repeatedly misread

requested flight levels, and mixed up FL360 (36,000 ft) with FL300 (30,000ft).

Others reported difficulties of seeing some letters clearly, particularly the Glasgow code EGPF and the Cardiff code EGFF.

NATS and the CAA (Civil Aviation Authority, U.K.) have said that difficulties in reading screens has been experienced only by a small number of controllers, and that it is not a safety matter. NATS also said that an improved display had been developed and a prototype was shortly to undergo testing.

The risks are many and unfortunately obvious. But what happened to the principles of good HCI design (human-computer interface) and user acceptance testing? Obviously no-one thought to ask the controllers if they could actually read the screens clearly as they play three-dimensional chess with the aircraft and passengers flying into, out of, and past one of the busiest airports in the world.

✶ Paper: How to own the Internet in your spare time

"Nicholas C. Weaver" <nweaver@CS.Berkeley.EDU>
Wed, 22 May 2002 12:38:44 -0700 (PDT)

Stuart Staniford, Vern Paxson, and I have completed our paper, "How to Own the Internet in Your Spare Time"
<http://www.cs.berkeley.edu/~nweaver/cdc.web/>
to appear in the 11th Usenix Security Symposium (Usenix Security

'02).

We've combined an analysis of Code Red I (which is still endemic on the net, with ~2000+ hosts still infected), the effects of Code Red II and Nimda, with the possibility of some new threats we have discussed before (Warhol strategies, Flash worms), and some we haven't (contagion worms, which are highly resistant to traffic analysis and similar detection strategies, and programmatic updates which represent a natural evolution in utility for worm writers). We then use this to make a case for a CDC-like institution to proactively develop defenses for such threats.

Nicholas C. Weaver nweaver@cs.berkeley.edu

✂ Credit-card data from wireless registers

"Laurenson, Jim" <JLaurenson@icfconsulting.com>

Wed, 22 May 2002 16:43:56 -0400

On May 1, MSNBC ran a story, "Best Buy closes wireless registers; Hackers say credit-card data vulnerable; other retailers at risk." It's still there at <http://www.msnbc.com/news/746380.asp>. But the story also says "An anonymous security researcher announced on a computer security research mailing list Wednesday that several U.S. retailers have made the mistake of installing wireless cash registers and transmitting the traffic in clear text, without encryption." So what's that other mailing list?

Jim Laurenson, ICF Consulting, JLaurenson@ICFConsulting.com *
<http://www.ICFConsulting.com>

✶ Ford Motor Credit office baffled by theft

"Dave Hansen" <iddw@hotmail.com>

Wed, 22 May 2002 16:49:40 -0400

Apparently, someone was able to steal credit reports from Experian by masquerading as Ford Motor Credit. They don't know how, but it won't happen again. Very confidence inspiring...

No further comment, just some excerpts:

Officials still aren't sure who, or how, someone snatched 13,000 credit reports through Ford Motor Credit Co.'s Grand Rapids office." What they are sure about, however, is that no more credit reports will be stolen -- at least from this group. "We're not sure how this happened, to be honest," said Melinda Wilson, spokeswoman for Ford Motor Credit. "We thought we had a tight system. We're going to have an even tighter system now." The reports provided the intruders with a wealth of information, such as Social Security numbers, credit ratings, account numbers for bank accounts and credit cards, and creditors names and payment histories, Experian said.

Full Story at

http://www.mlive.com/business/grpress/index.ssf?/xml/story.ssf/html_standard.xsl?/base/business-0/102199233690053.xml

(watch URL wrap).

⚡ Vending Machines - Poor Programming

"T.J. Griesenbrock" <ruritani@earthlink.net>

Wed, 22 May 2002 19:50:34 -0400

Oh, vending machines are the most defective thing I have ever seen in public service. Check around for a vending machine with a green/blue LCD screen, and a numeric pad using a telephone-style grid. Press 8.

Then press 2. Then quickly press 8 and 2 at the same time. It will crash, and reboot. Any money in the slot is 'forgotten.' An obvious sign of buffer overflow bug, or a sad case of a slow processor trying to keep up with an user's fast fingertips, as programmers tend to have. :)

Unfortunately, I do not remember to check for any identifying signs to distinct that model from any other models. Also equally unfortunate, I do not find any bugs that somehow reward the user instead of the vendors, implying that the developers were at least careful enough to prevent users from grabbing free grub.

⚡ RISKS of providing smart-alecky false information

"Daniel P. B. Smith" <dpbsmith@theworld.com>

Wed, 22 May 2002 20:06:51 -0400

At one time or another, I signed up for Passport--I believe because it was required to get the 90 days of free technical support with some software product or another. Recently, Microsoft decided to opt in every Passport user for information sharing.

I went to my Passport account to attempt to change it this preference, but found that I could not, because between the time when I first enrolled in Passport and now they have added a number of new personal information items--and (for some reason) it will not allow you to change ANY of the items unless you've entered ALL of them.

Naturally, I did what anyone would do--filled in all the blanks with bogus information. And while I was at it, I decided to change my first name to "Mickey," my last name to "Mouse," and my date of birth to 04/01/2001.

I unchecked the "Share Information" box and clicked the confirmation button. To my horror, a screen came up saying that because I was under thirteen I would need my parents' consent! I then received the following email:

"Dear Parent or Guardian:

Your child, Mickey Mouse, has registered for a Microsoft .NET Passport and needs your consent to sign in to a Kids Passport-participating Web site or service. Your child indicated that he or she is under 13, and according to U.S. law, Web sites and services that collect, use,

or
share visitors' personal information must obtain a parent or
guardian's
consent to allow children under 13 to sign in....

If you do not have a .NET Passport:

You need to have a .NET Passport in order to give or deny
consent. .NET
Passport is a free service from Microsoft that allows you to use
a
single e-mail address and password to sign in to a growing
number of
participating Web sites.

NOTE: To register as a parent or guardian, you will need to
verify that
you are at least 18. You can use a credit card to do this. Your
credit
card account will not be charged, and .NET Passport will not
retain or
share the information."

⚡ Phony 'soldier' needs your help giving him your money

"NewsScan" <newsscan@newsscan.com>

Thu, 23 May 2002 09:03:23 -0700

A scam e-mail message now circulating the Internet purports to
be from a
"Special Forces Commando" in Afghanistan who's found \$36 million
in drug
money while on patrol, and who wants your help in moving the
cash. Sure he
does. "We will thus send you the shipment waybill, so that you
can help
claim this luggage on behalf of me and my colleagues. Needless
to say the
trust in you at this juncture is enormous. We are willing to

offer you an agreeable percentage of funds." Stop laughing, and grab onto your wallet.

[AP/San Jose Mercury News 23 May 2002; NewsScan Daily, 23 May 2002]

<http://www.siliconvalley.com/mld/siliconvalley/3319360.htm>

[The Nigerian scams have been spawning numerous copycats, but this one is a new variant. PGN]

✶ Re: Fun with fingerprint readers ([RISKS-22.08](#))

Arnt Gulbrandsen <arnt@gulbrandsen.priv.no>

Thu, 23 May 2002 10:25:37 +0200

He tried eleven commercially available fingerprint systems and spoofed **all** of them (100%). The average single attempt had an 80% chance of success.

The reputable German magazine c't ran a cover story just now with similar claims. They tested 11 iris, face, and fingerprint recognition system and spoofed **all** of them. Some of their techniques were hilariously simple... it'll be a long time until this reader can take biometrics seriously.

[Quite a few readers noted my mistake in [RISKS-22.08](#). It has been corrected in the archives. Thanks to all of you. PGN]

✶ Re: 2 unsolved telephone mysteries (Goodman-Jones, [RISKS-](#)

22.08)

Stanislav Meduna <stano@meduna.org>

Wed, 22 May 2002 21:57:35 +0200 (CEST)

> How did her mobile phone make a call by itself at 5am?

I don't know Samsung phones, but does it have a quick-dial feature using a longer press of a key? I can well imagine some conductive piece of dirt or moisture "making" the call - these keypads are not very robust. It stopped before answering it because the calls get dropped by the switches if not answered in 1 minute or so (pretty normal at this time).

As to why at 5 am I have another story: Plain old alkaline batteries in one of my devices have the nasty habit of going empty early in the morning (the device tells it quite loudly). They seem to nearly always wait with their last breath until I sleep the best. My theory is that it is simply colder at this time and as the voltage correlates with the temperature, the most of the daily voltage drop occurs when the temperature also falls and so it is more probable that the warning is triggered at night.

If the quick-dial theory is right, a change in temperature could well be the triggering factor.

Sometimes there are connections where nobody expects them - this is often a risk.

> Here's the weird bit: A call at a very similar time was made on
> my HOME phone to the same number (which I don't recognise at all).

There are some obscure possibilities involving callback requests (possible in some networks) or redirecting calls, but this really smells like a problem of the phone company (either billing software, or worse - phreaking).

I heard of people finding missed calls from themselves on a mobile phone - and without an entry in the outgoing calls list.

✶ Re: 2 unsolved telephone mysteries (Goodman-Jones, [RISKS-22.08](#))

"Chris Barnabo" <chris@spagnet.com>
Wed, 22 May 2002 16:03:06 -0400

Gremlins in the mobile firmware? Unlikely - since caller-id typically doesn't pick up a telephone number until the `_second_` ring I suspect mum was awakened by a wrong number or a crank caller, and the mobile phone & caller id were simply showing a call completed earlier in the day (or perhaps the preceding day, given the time!)

✶ Re: Copy-Protected CDs (Arthur, [RISKS-22.07](#))

Jan Ingvoldstad <jani+comp.risks@ifi.uio.no>
23 May 2002 09:29:15 +0200

For one thing, they aren't copy protected, and for another, they

aren't CDs.

We should be careful about allowing Sony to call the disks "CDs", because that is making their stunt legitimate. We should also be careful about allowing Sony to call the scheme "copy protection", because it does not protect against copying, but rather against (presumably legitimate) use. Call it "usage prevention", "usage limitation" or other such.

> But it would seem that the folks that created the format in direct violation of published standards should share some of the blame and resulting liability.

If we choose to follow the line of thinking I mentioned above, we should also take the consequences when the disks are marketed without clearly specifying that they aren't CDs, or that they may possibly break your CD players if you do so; just labelling them with "Does not play on PC or Mac" is hardly sufficient. Return the disk to the vendor, asking for your money back. If it has damaged your equipment, require an adequate replacement or financial compensation for the damage. And if you're a US citizen, consider the possibility of a class action lawsuit.

✉ Re: Copy-Protected CDs (Bumgarner, [RISKS-22.08](#))

Sean A Dunn <sad@cyberlink.ch>
Wed, 22 May 2002 15:22:32 -0400

I agree that it can be considered unfair to PC manufacturers that CDs are being deliberately 'corrupted' in the name of Copy Protection. However, I am not convinced that liability should be considered to be anywhere other than with the PC hardware/software manufacturers when the PC crashes/freezes.

Why shouldn't either the hardware or OS handle the error when the CD is corrupted? After all, corruption could happen for other reasons. Even though it is extremely unlikely that a dirty/scratched/faulty CD will contain the stream of bits that cause the current problems, there should never be a case that can't be handled by the combination of PC hardware and operating system.

The good news for consumers: Surely it can't be long before PCs simply ignore the 'error' and carry on...

✶ Re: Copy-Protected CDs (Bumgarner, [RISKS-22.08](#))

Russ Perry Jr <slapdash@enteract.com>

Wed, 22 May 2002 21:28:19 -0500

I think in this case the liability is ENTIRELY in the hands of those making the discs.

Anyone with a modicum of smarts will know that ONLY gas should go into the gas tank. And even though we call it toilet "paper", most know that only

"real" paper goes into a printer.

But who would suspect that a CD shouldn't go into a CD drive?
It's worse
than someone trying to throw in a Playstation disc or a DVD.
Even BY NAME
it's the same thing. Unless there's a warning on the disc, and
in big
print, the people making the discs are simply inviting trouble
and
encouraging consumer problems. That ain't right.

And I'm sitting here facing the old Mac that IS my CD player;
haven't ripped
a single song with it, or my newer Mac, which would probably be
my new CD
player if the built-in speakers were better. So if one of these
discs
messes up my computer, when I had no intention or violating
copyright law,
you'd better believe that I'm not going to be happy at all.

How can you tell the regular CDs from these killer CDs?

Russ Perry Jr 2175 S Tonne Dr #114 Arlington Hts IL 60005
847-952-9729 slapdash@enteract.com

**[Re: Apple: break your new PC with a copy-protected CD ... \(R
22 07\)](#)**

Martin Ward <Martin.Ward@durham.ac.uk>
Thu, 23 May 2002 10:02:07 +0100 (BST)

Who's fault is it if a service station starts selling petrol
(gas)
containing a significant percentage of sugar solution?
Especially if said
garage does not give any indication that their product is any

different from
that which is for sale at every other station?

Note that these copy-protected CDs are deliberately designed
not to work
in a PC. If the PC manufacturer "fixes" their machines so that
the CDs
will work, then they will be in violation of the DMCA.

Martin.Ward@durham.ac.uk <http://www.cse.dmu.ac.uk/~mward/> Erdos
number: 4

✉ Re: More on Klez (Mech, [RISKS-22.07](#))

Joseph Brennan <brennan@columbia.edu>
23 May 2002 11:49:44 -0400

> To my experience, the Return-Path header generally contains
the infected
> person's address, or enough of a clue that you can narrow down
the
> listmember[0] who might be infected.

I have yet to see a single case where the Return-Path (that is,
the smtp
"mail from:") is the real sender. On the contrary, we are
rejecting 400,000
relay attempts a day pretending to be our users sending mail.
When we
detect campus hosts sending Klez, the logged "mail from:" has
never been the
address of the owner of the PC.

The biggest fallout problem is anti-virus programs smart enough
to recognize
Klez but not smart enough to know the sender is always faked.
For Klez,
sending a "helpful" notice to the apparent sender is a really

bad idea. It adds to the problem, not to the solution. The only useful notice would be to postmaster or abuse at the host that sent the message. We can filter Klez; it is almost impossible to filter the varying notices that anti-virus programs send, so they ironically are now the biggest headache for support staff.

Joseph Brennan Postmaster Academic Information Systems
Columbia University in the City of New York postmaster@columbia.edu

⚡ REVIEW: "Cyber Forensics", Albert J. Marcella/Robert S. Greenfield

Rob Slade <rslade@sprint.ca>
Mon, 20 May 2002 20:25:10 -0800

BKCYBFOR.RVW 20020319

"Cyber Forensics", Albert J. Marcella/Robert S. Greenfield, 2002, 0-8493-0955-7, U\$49.95
%E Albert J. Marcella
%E Robert S. Greenfield
%C 823 Debra St, Livermore, CA 94550
%D 2002
%G 0-8493-0955-7
%I Auerbach Publications
%O U\$49.95 +1-800-950-1216 auerbach@wgl.com orders@crcpress.com
%P 443 p.
%T "Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes"

The introduction to this book emphasizes the fact that this is a

field

manual, designed for quick reference, and not a textbook for study.

Unfortunately, the authors seem to have taken this as licence to throw in

all manner of random text and documents, without much structure or thought

for the user.

Section one outlines the various aspects of cyber forensics, according to

the book's definition. Chapter one is entitled "The Goal of the Forensic

Investigation," but the actual contents offer both more and less than that.

The chapter starts with a few possible specific investigations, and provides

directions on initial questions to ask. When the material moves to more

general discussion of investigations, it becomes vague, and loses utility.

Non-liturgical investigation (one that is not expected to end up in court)

is examined in chapter three, even though the text admits that the procedure

should be the same whether you expect to end in court or not: just collect

everything you can. The content is limited to Windows, and specifically to

the use of Internet Explorer. Much the same, with a little additional

material on the Registry and event log, is done with liturgical investigations in chapter three. A repetition of the same information about

Internet Explorer cache and cookies is found in chapter four. Chapter five

describes nmap, and its author, in some detail, and then lists a number of

other UNIX utilities. The broadest possible interpretation of intrusion

investigation is discussed in chapter six, and, again, the advice boils down

to the importance of careful collection of all possible

information.

Chapter seven outlines rules of and considerations for evidence in US courts of law.

Section two expands on this last chapter, looking at US (and supposedly international) statutes. Chapter eight examines US law regarding the admissibility of evidence intercepted from communications or recovered from seized computers. Changes to the US National Information Infrastructure Protection Act, and an editorial stating that cybercrime is bad, are given in chapter nine. The preamble to, and some questions about, a draft of the Council of Europe Convention on Cybercrime, are reproduced in chapter ten. Chapter eleven contains random comments on privacy. US Presidential Decision Directive 63, calling for a plan for protection of information infrastructure, and a speech justifying the use of Carnivore are reprinted in chapter twelve. Chapter thirteen replicates an overview of US Public Law 106-229 on electronic signatures (E-SIGN) as well as a number of other pieces relating to electronic commerce. Legal considerations in providing the electronic systems mandated by the US government paperwork reduction act are discussed in chapter fourteen. Speeches and comments on the US government's attitude towards encryption are given in chapter fifteen. Chapter sixteen looks at various pieces of US legislation related to copyright.

Section three concerns tools for forensic investigation. Chapter seventeen

discusses such tools in a very generic way, and then briefly lists a number of specific programs. There is a two page list of FBI office phone numbers in chapter eighteen, which is supposed to guide you in reporting Internet-related crime. Chapter nineteen is a simplistic four page list of questions to ask when conducting a computer audit.

This is definitely not a field manual. It offers almost no practical advice on collecting evidence from computers: if the material in this book is helpful to you, you have too little knowledge of the technology to have any business being engaged in computer forensics. The most valuable part of the book involves the collection of documents regarding US computer related legislation, but that would be of interest only to American lawyers. It would be difficult to recommend this work to anyone else. Even security personnel wanting a background on US federal legislation might be advised to look elsewhere, since the lack of structure and analysis in the book makes it very hard to read.

copyright Robert M. Slade, 2002 BKCYBFOR.RVW 20020319
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

<http://victoria.tc.ca/techrev> or <http://sun.soci.niu.edu/~rslade>



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 10

Monday 27 May 2002

Contents

- [US Navy suffers domain hijacking](#)
[Geoffrey Brent](#)
- [California personnel files were breached for 265,000 workers](#)
[Monty Solomon](#)
- [Face recognition kit fails in Fla airport](#)
[Thomas C Greene via Dave Farber](#)
- [Dutch city implanting chips to monitor tree health](#)
[Sander Tekelenburg](#)
- [Risks of quoting command language in e-mail](#)
[Mich Kabay](#)
- [Glitch leads to huge airfare bargains](#)
[Jason Axley](#)
- [Re: Copy-Protected CDs](#)
[Alan J Rosenthal](#)
- [Re: Apple copy-protected CD](#)
[Benjamin Robinson](#)
- [Re: Ford Motor Credit office baffled by theft](#)
[Greg Searle](#)
- [Re: Vending Machines - Poor Programming](#)
[Ryan O'Connell](#)

- [Re: Candy machine punishes the quick-thinking](#)
[Alan P](#)
 - [Re: S-P-A-M-demonium](#)
[Klaus Johannes Rusch](#)
 - [Re: SpamAssassin + Vipul's Razor](#)
[Karsten M. Self](#)
 - [Re: 5am call](#)
[Gavin Treadgold](#)
 - [More on Klez](#)
[Simson L. Garfinkel](#)
[Jonathan Kamens](#)
 - [Klez and mail loops](#)
[Martin Pool](#)
 - [REVIEW: "CISSP All-in-One Certification Exam Guide", Shon Harris](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ US Navy suffers domain hijacking

Geoffrey Brent <g.brent@student.unsw.edu.au>

Mon, 27 May 2002 14:52:05 +1000

When the US Navy forgot to renew registration on NavyDallas.com - apparently because Network Solutions forgot to send them a renewal notice - it was snapped up by a pornography site. NSI accepted the new registration despite the new owner being identified simply as "Bog". Meanwhile, NavyBoston.com now directs users to an eBay auction site:

<http://www.newsbytes.com/news/02/176741.html>

Porn hijacking is annoying, but at least it's pretty obvious. IIRC RISKS has previously mentioned some of the nastier things that can be done when someone has the opportunity to impersonate a 'trusted' domain, and allowing somebody to do so without even giving reasonable contact details looks like a recipe for trouble.

Geoffrey Brent - g.brent@student.unsw.edu.au

California personnel files were breached for 265,000 workers

Monty Solomon <monty@roscom.com>

Sun, 26 May 2002 14:35:16 -0400

Hackers gain entry to key state database
Ryan Kim, *San Francisco Chronicle*, 25 May 2002

Computer hackers have cracked into the state's personnel database and gained access to financial information for all 265,000 state workers, including Governor Gray Davis, officials said Friday. The database, housed at state's Teale Data Center in Rancho Cordova, holds names, Social Security numbers, and payroll information for everyone from office workers to judges. Authorities said that so far they have found no evidence that the information has been used illegally.

<<http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2002/05/25/MN179392.DTL>>

Face recognition kit fails in Fla airport

Dave Farber <dave@farber.net>

Mon, 27 May 2002 11:16:55 -0400

Thomas C Greene in Washington, The Register 27 May 2002

<http://www.theregister.co.uk/content/55/25444.html>

The face recognition system in experimental use at Palm Beach International Airport on 15 volunteers and a database of 250 snapshots. The success rate is less than 50%. Extrapolations also suggest a false-positive rate of about 50 passengers a day for a single checkpoint handling 5,000 passengers. "Eyeglasses gave the system a great deal of difficulty, in spite of copious Visionics marketing hype denying this particular glitch. Small rotations of the head, fifteen to thirty degrees off the camera's focal point, also bamboozled it repeatedly, and the lighting had to be just right."

[PGN-ed for RISKS. For Dave's IP archives see:

<http://www.interesting-people.org/archives/interesting-people/>]

✶ Dutch city implanting chips to monitor tree health

Sander Tekelenburg <tekelenb@euronet.nl>

Fri, 24 May 2002 02:49:04 +0200

Re: WashDC database crash linked to a death by a falling tree ([R_22_08](#)),

here is another computer angle on dead tree branches:

<http://nu.nl/document?n=57035> (dutch only)

[Loose translation] The Dutch city of Bloemendaal is going to implant chips in all its trees. With a portable computer, it will become easy to track the trees' health. The city thinks this will make tree maintenance cheaper and better, allowing trees to remain healthier and live

longer. Each chip contains a unique ID. Each tree's data is stored in a portable computer. The cost reduction is in not having to carry big stacks of paper and maps around while monitoring trees' health. More can be done in less time, and it will be easier to track exactly what maintenance was applied to which tree. Added bonus is that when a dead branch drops on a car, the city will be able to show that this was not caused by lack of maintenance. Cost of implanting all trees with these so-called "transponders" is 56.722 euro.

Sander Tekelenburg, <<http://www.euronet.nl/~tekelenb/>>

[Note that linguistically, a "transponder" is anything that works across the pond (familiarily, the Atlantic Ocean). PGN]

⚡ Risks of quoting command language in e-mail

Mich Kabay <mkabay@compuserve.com>

Fri, 24 May 2002 08:09:38 -0400

In a newsletter sent to 40,000 recipients, I included a block of HTML code showing a forged header.

The e-mail list software spotted what it thought was the end of the document and inserted the e-mail address of each recipient in that person's copy of the newsletter, making many readers believe that their e-mail address had been distributed to the entire list. Result: hundreds of letters (some nice, some not).

LESSONS:

(1) When designing macros that scan for search strings associated with a particular condition (in this case, the end of a message), it would be wise to test the presumption that the condition is in fact true. In this example, perhaps a second check might verify that there is in fact no further text in the message before inserting the valediction.

(2) When quoting control language (in this case, HTML), and in the absence of some sort of escape character (meaning "the following is literal text, not command language"), we may avoid accidents by using symbol substitution to prevent accidental misreading of the quoted strings as if they were actually to be interpreted.

M. E. Kabay, PhD, CISSP -- AssocProf Information Assurance,
DeptCompInfoSys,
Norwich University, Northfield VT <http://www2.norwich.edu/mkabay/index.htm>

✶ Glitch leads to huge airfare bargains

Jason Axley <jason-risks@axley.net>
Wed, 15 May 2002 07:43:23 -0700

``For about 45 minutes on 14 May 2002, visitors to the United Airlines Web site were able to buy roundtrip tickets for \$25. United blames it on an error by a computer that distributes fares for major airlines... It's not

the first time United has sold \$25 tickets on its site. In January, 142

passengers bought tickets to international destinations for as little as \$25.''

However, from the article, it sounds like it may have been due to human error, because ATP Co., the clearinghouse that distributes new sale fares to their Web site, was trying to fix a problem where a \$5 online discount was not reflected in the sale prices but ended up loading all prices but the actual fare itself. So the \$25 includes just the "taxes, facility charges and a \$5 surcharge".

Full story:

<http://www.cbsnews.com/stories/2002/05/15/national/main509107.shtml>

✶ Re: Copy-Protected CDs (Dunn, [RISKS-22.09](#))

Alan J Rosenthal <flaps@dgp.toronto.edu>

Fri, 24 May 2002 09:38:07 -0400 (EDT)

I strongly disagree. The CD is not "corrupted"; it contains an additional data partition, with malware on it. It is a trojan horse, because you execute that malware when you are trying to do something else. It prevents normal use of the CD (playing it for one's listening pleasure in a CD player, if that CD player is controlled by a computer).

I've listened to audio CDs on computers a handful of times, not

many; but I've never extracted any audio data from them, because I don't need to because I already have the data (on CD). I imagine that a great many RISKS readers are in a similar situation, as are the majority of the victims of these malware CDs. It prevents the regular use of the product with the consumer's choice of equipment, like any "embrace and extend" technological maneuver.

✶ Re: Apple copy-protected CD (Arthur, [R 22 07](#))

"Benjamin Robinson" <ixion@digital.net>

Fri, 24 May 2002 23:09:22 -0400

Apple has apparently softened their original position. I followed the link provided in the article, and found this end note, instead:

If a disc with copyright protection technology remains inside the drive after following the procedures above, or if the computer does not start up normally, it is recommended that you contact an Apple Authorized Service Provider (AASP) or Apple Technical Support. Audio discs that incorporate copyright protection technologies do not adhere to published Compact Disc standards. Apple designs its optical disc drives to support media that conform to such standards.

No mention of repair fees or the like, so I'll assume they will cut users some slack the first time they bring in their machines for service.

Benjamin Robinson bjr7@freenet.tlh.fl.us

✦ **Re: Ford Motor Credit office baffled by theft (Hansen, [RISKS-22.09](#))**

"Greg Searle" <greg_searle@hotmail.com>

Fri, 24 May 2002 12:41:59 -0400

How's this for a possible scenario?

- A Ford employee walks away from a workstation without locking it first.
- A watchful contractor/employee/visitor/whoever walks up to the system with
 - a prepared, custom-burned CD in hand.
- S/he pops the CD in, and an autorun program loads and immediately ejects the CD.
- The perpetrator takes the CD, closes the tray, and walks away within 10 seconds of approaching the workstation.
- The program that was just loaded goes to work in the background.
- The original employee returns with a fresh cup of coffee and resumes working, unaware that anything has happened.
- Later, at home/cafe/wherever, this person connects to the zombified system
 - (which has opened a path to itself through the firewall) and gets busy.

Sound farfetched? No. Any programmer with the proper motivation (13,000 credit reports are very motivating), a few bits of publicly-available developer knowledge, a simple development system, and a cheap CD-R drive could do just that. All firewalls have the same basic

weaknesses that can be taken advantage of, as long as the activity initiates from inside. The most secure Internet connection is no Internet connection at all.

This is all just informed speculation, but an office is only as secure as the weakest habits of its employees.

Re: Vending Machines - Poor Programming (Griesenbrock, Risks 22.09)

"Ryan O'Connell" <ryan-risks@complicity.co.uk>
Thu, 23 May 2002 20:03:11 +0100 (GMT Daylight Time)

This reminds me of an incident that happened not too long ago on the University campus (in the UK) that I attended. The vending machines on campus were the style where you can't see the item (Chocolate) before it is dispensed - you dial a two digit number and it gives you the product or tells you it's out of stock or how much it costs as appropriate. The machines usually had about 10 varieties of chocolate/chewing gum in them, so the valid entries were typically in the range 10-19 although some had more or less choices.

It seems some of the machines had been misprogrammed and some debt-ridden students had discovered that some of the higher numbers (80+) dispensed chocolate with the incorrect prices. Some of these prices were very high but others were ridiculously low - a few pence (less than 10 cents)

per
item. Some even had a zero value!

As you can imagine, it does not take long for news like this to spread and very quickly everyone knew if you wanted free or cheap chocolate and didn't care what you got then you could just walk up to the nearest machine and start punching buttons at random until you got something.

What is even more surprising is that the engineers that came to fill the machines with food and empty the cash did so several times before someone actually came along (A different engineer) and reprogrammed all the machines to fix this problem. I'm surprised this problem hadn't been discovered before at other sites, so I suspect either we had a badly setup batch of machines or the problem was known about but they didn't have the resources to reprogram every machine just in case.

The Risks here are obvious - as with almost every other Risks item, buggy software doesn't just cause bad PR, it can cost money!

⚡ Re: Candy machine punishes the quick-thinking (Rice, [RISKS-22.08](#))

arp <alanp@prism.co.za>
Thu, 23 May 2002 09:18:57 +0200

FYI, here is some info on the architecture of (admittedly older) vending machines:

Consists of the executive (typically the note acceptor/coin box) which controls the peripherals (typically the dispenser which also displays prices and come-on message, accepts your selection choice and vends the products). All these components are separate devices communicating via a shared bus. The executive controls the peripherals via a query-response protocol (either Protocol A or the newer MDC protocol). Neither of these protocols are particularly well-define in terms of exception handling. Moreover, manufacturers' implementation of these protocols can differ significantly (what a surprise).

The executive will tell the dispenser, for example, how much credit is available and when to vend (but not what to vend). If memory serves, the protocols define the acceptable states of a peripheral. E.g., the dispenser may not vend until it has received a 'credit' message. If one selects a product before the dispenser has received such a message the dispenser will (usually) display the product's price.

I'll leave it as an exercise to the reader to find as many RISKy (<groan>) scenarios as (s)he can with this setup.

>The risks? I suspect that the software that went in to the machine was
>tested by the programmer and not tested in the field before being released
>-- though the only way to find out would be to ask. Not doing real-world
>testing is a common risk but this fault was dumb and should have been easy
>to catch before the software was released.

Hhmmm...i'm not so sure. As for all timing-related errors (such as this), testing for them reliably can be tricky. Even worse is the differences between different manufacturer's vending peripherals (and their 'adherence' to the vending protocol). We've had the situation where our executive works reliable in 2 different types of vending machines only to fail horribly in the third type (from the same manufacturer).

```
> [Just wait until the thing starts accepting debit and credit
cards. More
> good ways to make the software fail! }:-} ]
```

The company I currently work have an executive that uses a smartcard as the payment token (in a closed payment system). At least this method has the advantage of being offline (i.e. doesn't have to communicate with a bank to authorise the payment) which supposedly reduces the risks of fraud (hah!).

✶ Re: S-P-A-M-demonium (Kevin, [RISKS-22.09](#))

Klaus Johannes Rusch <KlausRusch@atmedia.net>
Thu, 23 May 2002 21:50:26 CET

Of course there is an obvious risk with Vipul's Razor: corruption of the black list, either by accident -- it just takes a single provider to pipe all mails through the reporting script -- or on purpose, to prevent others from receiving a certain message, such as a virus warning.

Collaborative filtering with trusted co-readers can be very helpful, not just for spam tagging but general rating of information, yet I prefer to not let every stranger in the world filter my e-mail.

Klaus Johannes Rusch KlausRusch@atmedia.net <http://www.atmedia.net/KlausRusch/>

✉ Re: SpamAssassin + Vipul's Razor (Re: Kevin, [RISKS-22.09](#))

"Karsten M. Self" <kmsself@ix.netcom.com>
Sat, 25 May 2002 15:18:44 -0700

As a ***VERY*** happy customer of SpamAssassin, I was interested to see you've adopted it for the RISKS list.

Note that Kevin's (nobody@tex.kom) advice should not be necessary -- SpamAssassin already incorporates (and scores appropriately) information from the Vipul's Razor system.

✉ Re: 5am call ([RISKS-22.08](#))

"Gavin Treadgold" <gav@rediguana.co.nz>
Sat, 25 May 2002 15:58:08 -0400

> How did her mobile phone make a call by itself at 5am?

I have had a similar event occur, and often it is related to the

phone call
blocking caller ID. Take my cell phone, a Nokia 6210 for
example. It has
caller ID capability here in New Zealand. If the number is not
blocked, it
will display the number and log in a register of the 10 most
recent
received/missed numbers. If the number is blocked, then it is
not added to
the register. However, if you miss a call, it will provide a
'list' command
that will display the number of the most recently missed call
from the
missed call register. This works fine if last call had a called
ID number
that was added to the missed calls register. If the last call
had a blocked
caller ID, then no number was added to the top of the register,
and if you
hit list, the top of the register displays the last valid caller
ID number
before that.

So all that had to happen was for you mum's last recorded caller
ID call to
be from her mobile to her home, and then then next call to be
from a caller
ID blocked phone, and it is possible that the displayed number
was the last
previous identifiable number, rather than the last actual call.
Of course
this depends on her caller ID unit, and what I've noted from my
cell phone,
my not be applicable towards her caller ID unit.

More on Klez

Simson L. Garfinkel <simsong@vineyard.net>

Sat, 25 May 2002 12:33:37 -0400 (EDT)

Largely as a result of the previous postings on this list, I decided to get my act together and re-install the anti-virus scanning for my ISP. (The last time I turned it on, a configuration error caused the anti-virus to eat several thousand email messages, so in the meantime I had developed some automated email testing tools.)

In any event, I'm stunned. My ISP has less than 1500 active mailboxes, but we're receiving several copies of W32/Klez-G per minute. Some users are actually receiving 30-60 copies of this virus every day. (Hopefully they are running their own anti-virus...)

It just goes to show the danger of a monoculture.

More than 50% of the viruses are being sent by one or two people who have cable modems. It makes you wonder if there should be any liability for these individuals.

✶ Re: More on Klez (Brennan, [RISKS 22.09](#))

Jonathan Kamens <jik@kamens.brookline.ma.us>

Thu, 23 May 2002 15:33:30 -0400

This is very strange, because I have had exactly the opposite experience. I have one confirmed case of the envelope address indicating the actual sender of the infected message -- the envelope sender matched up with the Received

lines, and when I spoke to the envelope sender, who is a friend in town and thus easily reachable, he confirmed that his computer was infected.

In the vast majority of the other copies of this virus I've received, the envelope sender has matched up with the Received lines, and none of the so identified individuals whom I've contacted have responded with a claim that their machines were actually not infected (although they also have not responded to confirm that they *were* infected).

Perhaps there is a new Klez variant that I haven't yet seen, which forges the envelope sender as well?

⚡ Klez and mail loops

Martin Pool <mbp@sourcefrog.net>
Thu, 23 May 2002 15:49:37 +1000

A machine I co-administer recently suffered what at first looked like a mailbomb attack. On further investigation, it seems that it was probably a side effect of the Klez worm, possibly unintended but rather destructive.

As was explained in a previous issue, the Klez family send e-mail from an infected computer A to an address B, with the From address forged as a third party C. B and C are selected apparently at random from the address book of A, or possibly other sources.

Any bounce messages caused by the attempted delivery to C will be sent to B. Readers will probably have suffered over the last month mailboxes full of not just Klez worms but also bounce messages or auto-generated virus warnings. (Incidentally, one might hope that e-mail anti-virus vendors would be smart enough to send notifications to A rather than B in this case, but apparently many are not.)

If both addresses B and C are configured to auto-reply to messages, then a rather more destructive mail loop can occur, producing network traffic and also filling mailboxes or databases at both ends. In the particular attack we observed, B was a robot that sent instructions about an FTP archive, and C was a bug-submission address that sent automatic acknowledgements.

Of course, mail loops are always a risk when programs automatically generate e-mail. They can be avoided if either program is sufficiently smart to detect and break the loop: the BSD vacation program, and most mail transports agents do this quite well, for example. However, many other programs can't detect loops under some circumstances, particularly if the other party is also somewhat RFC-ignorant: for example, if it drops the X-Loop header, or does not set a Precedence or Sender appropriately.

"Untested code is broken code", and many of these bugs have never been thrown up because bug databases don't normally get into arguments with FTP robots. Because Klez picks addresses apparently at random, it

kicks off

interactions between programs that might never normally occur.

In general, the most likely situation for an autoresponder loop is probably

an SMTP bounce message, but since most mailers try to avoid loops the

autoresponder can get away with only simple checks for loops.

When two such

robots talk to each other, loops can easily occur.

Interestingly, the machines most affected by the event need not be

vulnerable to the worm, or even running Windows at all! Like some previous

DDOS attacks, the disruption is amplified by the autoresponders, so A sends

only one message to start the chain reaction.

It seems that some mail autoresponders need to be better defended against

conversations with poorly-designed or malicious remote parties. Countermeasures might include setting the reply address to one that will not

cause more mail to be sent, and using a global or per-address rate limit.

★ REVIEW: "CISSP All-in-One Certification Exam Guide", Shon Harris

Rob Slade <rslade@sprint.ca>

Mon, 27 May 2002 08:19:40 -0800

BKCISPA1.RVW 20020503

"CISSP All-in-One Certification Exam Guide", Shon Harris, 2002, 0-07-219353-0, U\$79.99

%A Shon Harris shonharris@hotmail.com

%C 300 Water Street, Whitby, Ontario L1N 9B6
%D 2002
%G 0-07-219353-0
%I McGraw-Hill Ryerson/Osborne
%O U\$79.99 905-430-5000 +1-800-565-5758 fax: 905-430-5020
%P 971 p. + CD-ROM
%T "CISSP All-in-One Certification Exam Guide"

Chapter one is a very reasonable review of the CISSP (Certified Information Systems Security Professional) credential, and the (ISC)² (International Information Systems Security Certification Consortium) exam process, including recertification. As with most of the chapters in the book, it has a set of sample questions, and while I could quibble with some, they cover a decent range of topics and a representative extent of difficulty. There are resources listed in this and other chapters, mostly Web sites. Web sites are, of course, most easily accessible, but they also die on a regular basis, and it might have been an idea to include references to other books on specific topics. It is difficult to see the point of chapter two--an opinion-piece level overview of various security related topics.

Chapter three begins the first of the ten domains of the Common Body of Knowledge (CBK) with security management practices. It is obvious that the material has been structured and based on the (ISC)² CBK review course, even to the use of specific tables and diagrams, but the material is, at least, enhanced and extended by narrative discussion. Access control is explained clearly (and sometimes amusingly) in chapter four (although biometrics is generally considered to be a form of authentication, not identification). In general, the coverage of security architecture and models in chapter

five is quite useful. However, there is too much emphasis on the old "Orange Book" TCSEC (Trusted Computer System Evaluation Criteria) and not enough on the newer Common Criteria. (The inclusion of a section on computer hardware is also a bit odd.) Chapter six has many of the blind spots about physical security common to most computer security types (including some erroneous information about Halon from the old CBK course). The telecommunications and networking material, in chapter seven, presents the underlying concepts well, but for some reason fails to address many of the security technologies. The explanations of cryptography, in chapter eight, are problematic. Fortunately, the content is not necessarily wrong. The author obviously is not familiar with this area, and the text in such areas as DES (Data Encryption Standard) modes and one way encryption doesn't make sense, although it does not necessarily misinform the reader. Chapter nine, dealing with business continuity and disaster recovery, is reasonable, but not as detailed as other sections. Law, Investigation, and ethics is pretty good, although some old crimes and the insistence on the salami scam myth are some notable flaws in chapter ten. Chapter eleven, applications development, contains the basic information but does not always make the connections to security. Operations security gets a sensible review in chapter twelve.

The material is much more reliable and better structured than the SRV Press books (cf. BKCISPET.RVW), and much more reliable and complete than the Andress work (cf. BKCISPEC.RVW). Like the Krutz and Vines volume (cf. BKCISPPG.RVW) it is quite obvious that the content

and organization is copied from the old CBK course (sometimes slavishly), although Harris does put more explanatory and narrative substance into the text. (Interestingly, there are some indications that this is based on an even older version of the course than Krutz and Vines used.) Even considering the noted weak areas in this book, it should provide a reasonable basis as a study guide for the CISSP exam, although those who use only this work should not expect to get a particularly high mark.

copyright Robert M. Slade, 2002 BKCISPA1.RVW 20020503
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

<http://victoria.tc.ca/techrev> or <http://sun.soci.niu.edu/~rslade>



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

[ACM](#) Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 11

Thursday 6 Jun 2002

Contents

- [Impact of inadequate software testing on US economy](#)
[Rick Kuhn](#)
- ["Truncation error" found in GPS code on Int'l Space Station](#)
[George White](#)
- [FBI's Carnivore hampered anti-terror probe](#)
[Marc Rotenberg](#)
- [Sex, Truth and Videotaping](#)
[Gary Marx](#)
- [Kursk submarine: to test or not to test ...?](#)
[Ken Knowlton](#)
- [Deja vu: Stockholm power outage hits high-tech companies](#)
[Ulf Lindqvist](#)
- [Inadvisable instructions from Sun on StarOffice 5.2](#)
[John Sullivan](#)
- [Confirming cricket score reason for delay](#)
[R. Jagannathan](#)
- [Students provide bulk of tech support in schools](#)
[NewsScan](#)
- [More on typos and homographs](#)
[Martin Wheatman](#)

● [Please ignore the anti-shoplifting device!](#)

[Mario Hendricks](#)

● [Re: The Klez Effect](#)

[Paul van Keep](#)

[Greg Searle](#)

● [Re: Klez and mail loops](#)

[A. Harry Williams](#)

● [More on Klez](#)

[Hal Lewis](#)

● [Info on RISKS \(comp.risks\)](#)

✶ Impact of inadequate software testing on US economy

Rick Kuhn <kuhn@nist.gov>

Wed, 05 Jun 2002 14:53:35 -0400

NIST has released a new study conducted by the Research Triangle Institute that should be of interest to readers: "The Economic Impacts of Inadequate Infrastructure for Software Testing". Comments and discussion are welcome.

<http://www.nist.gov/director/prog-ofc/report02-3.pdf>

Rick Kuhn

From the summary:

NIST engaged the Research Triangle Institute (RTI) to assess the cost to the U.S. economy of inadequate software testing infrastructure. Inadequate testing is defined as failure to identify and remove software bugs in real time. Over half of software bugs are currently not found until downstream in the development process leading to significant economic costs. RTI

identified a set of quality attributes and used them to construct metrics for estimating the cost of an inadequate testing infrastructure. Two in depth case studies were conducted. In the manufacturing sector, transportation equipment industries were analyzed. Data were collected from software developers (CAD/CAM/CAE and product data management vendors) and from users (primarily automotive and aerospace companies). In the service sector, financial services were analyzed with data collected again from software developers (routers and switches, financial electronic data interchange, and clearinghouse) and from users (banks and credit unions). ...the annual cost to these two major industry groups from inadequate software infrastructure is estimated to be \$5.85 billion. Similarities across industries with respect to software development and use and, in particular, software testing labor costs allowed a projection of the cost to the entire U.S. economy. Using the per-employee impacts for the two case studies, an extrapolation to other manufacturing and service industries yields an approximate estimate of \$59.5 billion as the annual cost to the nation of inadequate software testing infrastructure.

✶ "Truncation error" found in GPS code on Int'l Space Station

George White <aa056@chebucto.ns.ca>
Thu, 30 May 2002 08:45:11 -0300 (ADT)

The following excerpt describes the resolution of a problem in the GPS attitude control for the International Space Station.

> From j.vanoene@chello.nl Thu May 30 08:28:31 2002
Date: Wed, 29 May 2002 06:43:17 -0700
From: Jacques van Oene <j.vanoene@chello.nl>
Newsgroups: sci.space.news
Subject: ISS On Orbit status 28-05-2002

"The troubleshooting of the GPS (global position system) attitude errors has been successful. At first thought to be due to the high solar Beta angle (where fewer GPS satellites are in sight), the cause has now been traced to the software, which did not calculate attitudes correctly due to a truncated parameter. The error was eliminated, and the system is now working fine, even at high Beta angles, supplying state vector and attitude data. With Russian concurrence, GPS will now also provide the periodic updates of the SM's BINS strapdown navigation and guidance system, instead of requiring lengthy manual data takes by the crew using the optical PUMA system, thus saving valuable crew time."

Not to mention the psychological benefits to the crew of one less "area of concern" in a setting where resolving glitches in a critical subsystem can easily become an exercise in "staying alive".

George White <aa056@chebucto.ns.ca> Halifax, Nova Scotia

🔥 FBI's Carnivore hampered anti-terror probe

Marc Rotenberg <rotenberg@epic.org>

Tue, 28 May 2002 17:03:50 -0400

FBI'S CARNIVORE SYSTEM DISRUPTED ANTI-TERROR INVESTIGATION
INTERNAL MEMO CALLS OVER-COLLECTION OF DATA PART OF "PATTERN"
SHOWING

"INABILITY OF THE FBI TO MANAGE" FOREIGN INTELLIGENCE
WIRETAPS

Washington, DC -- An FBI anti-terrorism investigation possibly involving Usama bin Laden was hampered by technical flaws in the Bureau's controversial Carnivore Internet surveillance system. The incident, which occurred in March 2000, is described in newly-released FBI documents obtained under court order by the Electronic Privacy Information Center (EPIC). A written report describes the incident as part of a "pattern" indicating "an inability on the part of the FBI to manage" its foreign intelligence surveillance activities.

An internal FBI e-mail message dated April 5, 2000, and sent to M. E. (Spike) Bowman, Associate General Counsel for National Security Affairs, recounts how the Carnivore "software was turned on and did not work correctly." The surveillance system captured not only the electronic communications of the court-authorized target, "but also picked up E-Mails on non-covered" individuals, a violation of federal wiretap law. According to the Bureau document, the "FBI technical person was apparently so upset that he destroyed all the E-Mail take, including the take on [the authorized target]."

The botched surveillance was performed by the FBI's

International Terrorism

Operations Section (ITOS) and its "UBL Unit," which refers to the government's official designation of bin Laden. The Bureau document

indicates that an official at the Justice Department's Office of Intelligence Policy and Review (whose name has been deleted) became aware of

the problem, and "To state that she is unhappy with ITOS and the UBL Unit

would be an understatement of incredible proportions."

The reported problem apparently was not the first to arise during the course

of FBI implementation of the Foreign Intelligence Surveillance Act (FISA).

The internal document concludes its report of the "UBL Unit" incident by

noting, "When you add this story to the FISA mistakes covered in [another,

unreleased document], you have a pattern of occurrences which indicate to

OIPR an inability on the part of the FBI to manage its FISAs."

Two Bureau documents written one week later discuss Carnivore's tendency to

cause "the improper capture of data," and note that "[s]uch unauthorized

interceptions not only can violate a citizen's privacy but also can

seriously 'contaminate' ongoing investigations" and that such interceptions

are "unlawful." An FBI lawyer (whose name has been deleted) writes that the

Bureau must "go out of our way to avoid tripping over innocent third party

communications." The lawyer concludes, "I am not sure how we can proceed to

test [Carnivore] without inadvertently intercepting the communications of

others, but we really need to try."

The Bureau lawyer notes that "missteps under FISA lead to mandatory

reporting to the President's Foreign Intelligence Advisory Board, and such errancies must be reported/explained/justified to Congress." The documents do not indicate whether the "UBL Unit" incident was reported to either body.

Since its existence became public in 2000, the Carnivore system has been criticized by EPIC and other privacy groups, as well as members of Congress, because it gives the FBI unprecedented, direct access to the data networks of Internet service providers. The FBI has publicly downplayed the system's potential for over-collection of private communications, although internal documents released earlier to EPIC confirmed such a risk. An independent review of Carnivore commissioned by the Justice Department also found that the system is capable of "broad sweeps" and recommended technical changes to address the problem. Neither DOJ nor the FBI has indicated publicly whether those recommendations were ever implemented.

The newly-released FBI documents were provided to EPIC on 24 May 2002, in response to a court order issued by U.S. District Judge James Robertson in the privacy group's ongoing Freedom of Information Act lawsuit seeking the disclosure of material concerning Carnivore. The order directed the Bureau to conduct a second search for relevant documents after EPIC successfully argued (over the Bureau's objections) that an initial FBI search was inadequate and likely overlooked responsive records.

The case is being litigated by EPIC's General Counsel, David Sobel, who

said, "These documents confirm what many of us have believed for two years -- Carnivore is a powerful but clumsy tool that endangers the privacy of innocent American citizens. We have now learned that its imprecision can also jeopardize important investigations, including those involving terrorism." Sobel added, "As we suggested when it first became public, Carnivore's use should be suspended until the questions surrounding it finally can be resolved. Our FOIA lawsuit shows that there's a great deal about Carnivore that we still don't know."

The newly-released FBI documents are available at:

<http://www.epic.org/privacy/carnivore/>

Contacts: DAVID SOBEL 202-483-1140 x105 WAYNE MADSEN x104

Sex, Truth and Videotaping

"gtmarx" <gtmarx@bainbridgeisland.net>
Tue, 28 May 2002 20:45:20 -0700

At-Home Spying: Privacy Wanes as Technology Gains
Surveillance may be legal, but is that the only standard?
Commentary by Gary T. Marx, 28 May 2002, *Los Angeles Times*
[Reprinted with the permission of the author]

Recently in France, a father who was concerned about the possible mistreatment of his 3-year-old son by a baby-sitter's boyfriend hid a miniature camera in his home to record any suspicious behavior. The father found some, but it was not abuse of the child; the camera

revealed the
baby-sitter and her boyfriend amorously entangled while the
child slept
soundly in the next room.

The father paid a penalty. In France, such videotaping is a
violation of
criminal and civil law. The father was arrested and ordered to
pay a fine
for invasion of privacy.

Did the father do something wrong? Is there a victim here? As
the ubiquitous
advertisements for cameras concealed in teddy bears and other
unlikely
places remind us, parents have an obligation to protect their
children. A
hidden video camera offers an easy way to do this--to the extent
that seeing
is believing. If nothing is found, the responsibly vigilant
parents rest
well knowing that the child was not harmed. If something is
found, there is
tangible evidence for taking protective and even legal action.
Different
privacy standards characterize home and work, as well as areas
within
these. The baby-sitter after all was not filmed in her own home
but at her
place of work.

Yes, the French parents had alternatives. They could have
discussed their
concerns with the sitter, checked to see whether other employers
had had
problems with her, banned the boyfriend or simply found another
baby-sitter. If there are some grounds for doubt, why take a
chance by
spying? And, as it turns out, the law was on the baby-sitter's
side.

In the U.S., the employer largely sets the conditions of work.
To use the

French baby-sitter as an example, the camera was in the living room, not in a bathroom where the expectation of privacy would have been greater. The place and the video equipment belonged to the parents, and the baby-sitter willingly came to the home. The images weren't sold on the Internet, used as blackmail or stolen.

To cast the best light on the father, he wanted to have the evidence in hand before deciding to fire the sitter. The use of hidden cameras is hardly an uncommon or exotic means for this. And, had the father been living in the U.S. instead of France, in most jurisdictions he would have broken no law.

Yet this videotaping, even if well-intentioned and revealing nothing incriminating, is patently offensive. E.M. Forster captured this well in noting: "For it is a serious thing to have been watched. We all radiate something curiously intimate when we believe ourselves to be alone." Secretly recording people violates their dignity and can put the individual at an unfair strategic disadvantage.

We assume, or at least morally expect, that under ordinary circumstances behavior behind closed doors, in darkness and at a distance will be protected from the eavesdropping of third parties. We also have a right to assume that interaction and communication are ephemeral and transitory and are not subject to being captured and preserved through hidden video or audio means without our knowledge. Another unintended consequence is that

sometimes people seeking specific information--i.e., whether their child is being mistreated--may observe something even they didn't want to know.

In addition, remotely transmitted signals might be picked up by others in the vicinity. The behavior of the spy is thus doubly troubling. Not only is he invading the privacy of those he is watching, but he may unwittingly enable others to invade as well.

The fact that there is still a legal right to secretly record images in the U.S. does not mean that it is the right thing to do. We would do well to learn from the French the general principle of respect for private life, a principle that holds no matter what new technologies are offered to us that allow us to spy on others.

Gary T. Marx, a Massachusetts Institute of Technology emeritus professor, is the author of "Undercover: Police Surveillance in Comparative Perspective" (Kluwer Law, 1995). Web site: garymarx.net.

✶ Kursk submarine: to test or not to test ...?

Ken Knowlton <KCKnowlton@aol.com>
Thu, 30 May 2002 08:23:45 EDT

Another Hubble Telescope story, of sorts: *Time Magazine* (3 Jun 2002) reports that when the Russian submarine Kursk sank, 23 of the momentarily surviving crewmen rushed to the floating rescue capsule located in the rear.

But it failed to disengage. It had never been tested.

⚡ Deja vu: Stockholm power outage hits high-tech companies

Ulf Lindqvist <ulf@sdl.sri.com>

Thu, 30 May 2002 09:08:17 -0700 (PDT)

In [RISKS 21.27](#), Mar 15 2001, I reported about about a large and long-lasting power blackout in Stockholm, Sweden:

> A fire in a tunnel containing power cables caused a long-lasting
> blackout for 50,000 people and a large number of high-tech
> companies in several Stockholm suburbs. [...] The largest employer
> in the area, Ericsson, told 11,000 employees to stay at home
> Monday as their workplace had no power.

Guess what - something very similar happened again on May 29 2002 in the same tunnel, with roughly the same consequences. In a press release, the utility company Birka Energi claims that this is actually not exactly the same situation as last time. In March 2001, it was an 11 kV cable in the tunnel that caught fire, and they claim that the cause of that particular problem has been eliminated. This time, however, they received a ground fault indication on a 33 kV cable right before the fire. To their customers, who will be without power for a couple of days, that information will not make much of a difference.

The risk is a familiar one: addressing specific symptoms instead of the

underlying vulnerability. PGN's comment about tunnel vision is unfortunately still appropriate.

Ulf Lindqvist, System Design Lab, SRI International, 333 Ravenswood Ave, Menlo Park CA 94025-3493, USA +1 650 859-2351 <http://www.sdl.sri.com/>

✶ Inadvisable instructions from Sun on StarOffice 5.2

John Sullivan <john@kanargh.force9.co.uk>
Wed, 29 May 2002 23:29:30 +0100

I heard today that Sun are withdrawing the free download of StarOffice 5.2, so I went over to their website to investigate. Having downloaded the package (in this case a single .bin file which is actually an executable) I went to the installation instructions at:

<http://wws.sun.com/software/star/staroffice/5.2/get/download.html>

Here we are told:

Note for Linux and Solaris[tm] customers only:

It will be necessary for a chmod command to be executed to set read, write, and execute permission.

For example:

```
% chmod 777 *.bin
```

Once you have set the permissions, you can run the setup, and

StarOffice 5.2 will do the rest.

One hopes that anyone seriously likely to be at risk of exploit due to this would not be inexperienced enough to actually follow their instructions blindly!

However a sufficiently inexperienced user, even though they are most probably not running a system shared with an adversary capable of attacking them because of this, may well absorb that command as some sort of "magic rune" and issue it at other times in the future when the window of opportunity is much wider.

✦ Confirming cricket score reason for delay

"R. Jagannathan" <jagan@reactivenetwork.com>

Tue, 4 Jun 2002 00:48:23 -0700

http://www.cricket.org/link_to_database/ARCHIVE/CRICKET_NEWS/2002/JUN/012194_NATION_03JUN2002.html

An interesting article from a "dependability" standpoint. Mismatch between what a computer thought was the revised target and what the umpire manually computed caused a 20-minute delay during which the teams had to play without knowing the revised target. The game between India and West Indies was won by India and the West Indian captain later rued the fact that their team did not know the score for 20 minutes, which affected how they played. All this

for a one-run difference between the manual and computed calculation.

The Duckworth-Lewis method is an empirically-derived table (by the two mathematicians) to compute revised targets when a one-day cricket match gets shortened by rain or other similar disruptions.

🔥 Students provide bulk of tech support in schools

"NewsScan" <newsscan@newsscan.com>

Thu, 06 Jun 2002 08:48:37 -0700

Fifty-four percent of U.S. schools rely on students to provide technical support for their computer systems, according to a report titled "Are We There Yet?" (<http://www.nsbf.org/thereyet/index.htm>), released yesterday by the National School Boards Foundation. In 43% of the 811 districts surveyed, students troubleshoot for hardware, software and other problems, and 39% of the districts, students are tasked with setting up equipment and wiring. Nearly as many districts also report that students perform technical maintenance. The fact that students are providing so much hands-on assistance is viewed as a "win-win" situation by John Bailey, director of education technology for the Department of Education. Their tech savvy helps compensate for a dearth of tech support funding in school budgets and teachers who are "unevenly prepared for using technology as a tool for teaching and learning," according to the NSBF, which reports

that 69% of the survey respondents rated new teachers as average or novices in computer skills. The role reversal signals a shift in the relationship between teachers and students as online lessons become integrated into the school curriculum, says Anne Bryant, executive director of the National School Boards Association: "Teachers become the guide on the side, instead of the sage on the stage." [AP 5 Jun 2002; NewsScan Daily, 6 June 2002] <http://apnews.excite.com/article/20020605/D7JV8EP00.html>

✶ More on typos and homographs

Martin Wheatman <Martin.Wheatman@compaq.com>
Tue, 28 May 2002 11:52:02 +0100

I use a national bank in the UK called Lloyds TSB (which is a recent amalgamation of Lloyds Bank and the Trustee Savings Bank), and I'm naturally keen to use their online services. However, I misspelt the name earlier this year (www.llyodstsb.com), and was taken to the real www.lloydstsb.com. I didn't immediately spot the typing error until I noticed that the Webmaster, rather incompetently perhaps (if it were a real scam), was using a free Web host service (www.uk2.net), which displays the redirected Web site underneath their banner advertising free Web hosting (I use the same company as they do provide a good, cheap, "no frills" service). Writing a program to redirect traffic to the end service is trivial (no need to even

provide Web content!), as would filtering usernames and passwords.

It's slightly different to the homograph scam as it relies on the typist to make errors (ad htat nerver hapens!), rather than providing the links already embedded in Web content, and feeds off www.websiteswithreallylongnames.com , and probably the fact that there will (I suspect) be a lot more combinations of typos than homographs. Also, the simple (but probably unheeded) solution to display mixed character sets wouldn't work... :(One protection, in the UK at least, is to access commercial sites through the ".co.uk" domain which is managed by Companies House (effectively the Government), who will only allow registered companies to use their registered names. Ok, so you could register a company with the misspelt name, but I suspect that Companies House (and the company being scammed) will no doubt be interested in the reasons for the similar name (probably using the same mechanism as protection for trademark laws / passing off?).

P.S. As a responsible citizen, I notified my bank (it was rather scary!), and although the site is still registered it is no longer used to redirect traffic (whether these two events are linked, I still don't know - presumably the Bank is still bothered by adverse publicity).

⚡ Please ignore the anti-shoplifting device!

Mario Hendricks <mario.hendricks@lmco.com>

Thu, 06 Jun 2002 13:26:46 -0400

The other day I went into my local Apple store to buy an external floppy drive. On my way out of the mall to my vehicle, I decided to take the shortest route, through a nearby Eddie Bauer store. As I walked into the store, the anti-shoplifting device sounded an alarm. As there were no other people within 5 or 10 meters, I realized that my recent purchase (from Apple) must have set off the alarm. I also realized that the alarm would likely sound as I exited at the other end of the store.

When I got near the parking lot exit, I encountered an Eddie Bauer employee. Rather than to get accosted as attempting to shoplift by this employee, I decided to warn him that the anti-shoplifting device would probably sound as I exited. The employee saw that I was carrying an Apple Computer bag (they have very distinctive shopping bags) and responded along the lines of "Oh, yeah, stuff from Apple always set off the alarm." Sure enough, when I left the store the alarm sounded.

The risks of such a false positive alarm are obvious. The fact that employees know to ignore the alarm (in at least this one case) raises even more risks. Of course, if anyone should ever want to shoplift from this store, there seems to be a tested procedure. You would think that either the store's management or the anti-theft device manufacturer would be concerned about such issues.

✉ Re: The Klez Effect

"Paul van Keep" <paul@sumatra.nl>

Tue, 4 Jun 2002 10:43:54 +0200

Yesterday I received a bounce from risks@csl.sri.com because I 'allegedly' sent a Klez.H infected e-mail to Peter. Of course I didn't (I thoroughly removed Outlook from my system and only use Polarbar, a Java mailer). But the interesting side effect is that the virus firewall nicely bounces the message to me, first stripping the infection payload. But what doesn't get stripped is the document that Klez attaches to each mail it sends out. So with each bounce I get a nice bonus. The Klez e-mails with me as originator come from somebody who seems to be a designer. I now have a collection of three different jpgs with nice pictures of jewelry and home appliances. (S)he must also be a RISKS reader, the only link between me and the RISKS e-mail. The risk is that virus firewalls, by not stripping all attachments from infected e-mails, not only block viruses from spreading, which is good, but also help in distributing potentially sensitive documents to third parties.

P.S. I'm still waiting to get a nice Word document with good takeover information so I can do some serious insider trading

[Classic case of address spoofing. There are also lots of

spoofs allegedly from RISKS. Don't Believe a Word! PGN]

✶ Re: The Klez Effect

"Greg Searle" <greg_searle@hotmail.com>

Tue, 4 Jun 2002 16:36:39 -0400

Listmasters are really getting hit, but you don't need me to tell you that.

Just today, another list that I subscribe to urged its members to rid themselves of the virus.

There's good news, however. According to MessageLabs (<http://www.messagelabs.com/viruseye/>), Klez is finally starting to slowly recede. It peaked two weeks ago at about forty thousand viruses intercepted by the company per day. Now it's around 27K/day.

So far, I've only had a couple of firewalls send me warnings that I "sent" the virus. No live person ignorant of Klez's forged header has complained yet.

✶ Re: Klez and mail loops (Pool, [RISKS-22.10](#))

"A. Harry Williams" <HARRY@VM.MARIST.EDU>

Tue, 28 May 2002 09:26:18 EDT

In discussing the Klez virus/worm, Martin Pool makes a common mistake among

UNIX admins, assuming that what is available on their system in TCP/IP utilities accurately and completely implements RFC specs. X-headers are user-defined headers, and therefore cannot be an RFC network standard header. I just searched, and can only find Precedence: in RFC 2076, where it is defined as "non-standard, controversial and discouraged". The real problem is that these auto-responders, including many Out of Office programs, try to use the email Headers, rather than the envelope headers. A simple MAIL FROM:<> that was correctly honored would stop many loops, and that is its purpose.

✶ More on Klez (Garfinkel, [RISKS-22.10](#))

hal lewis <hlewis@physics.ucsb.edu>

Mon, 27 May 2002 19:27:19 -0700

>It makes you wonder if there should be any liability for these individuals.

Who needs to wonder? This is theft, pure and simple.



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

[ACM](#) Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 12

Monday 10 June 2002

Contents

- [Is there a law that says you have to watch commercials?](#)
[NewsScan](#)
- [Dim STARS](#)
[Peter B. Ladkin](#)
- [Questions about new STARS air-traffic computer system](#)
[Ian Macky](#)
- [COTS versus Bespoke ATC Systems](#)
[Peter B. Ladkin](#)
[Nancy Leveson](#)
- [Re: Swanwick](#)
[Peter B. Ladkin](#)
- [*NY Times* new zero-security password system](#)
[Martin Ward](#)
- [Tracking subway users by electronic fare card](#)
[Ngiam Shih Tung](#)
- [Kazaa users inadvertently share their private files](#)
[Nathan Good](#)
- [Web glitch exposed Fidelity accounts](#)
[Monty Solomon](#)
- [Hacker threat posed by Excel spreadsheets](#)

[Patrick O'Beirne](#)

● [Re: More on typos and homographs](#)

[Martin Wheatman](#)

[Scott Nicol](#)

● [Info on RISKS \(comp.risks\)](#)

⚡ **Is there a law that says you have to watch commercials?**

"NewsScan" <newsscan@newsscan.com>

Fri, 07 Jun 2002 09:31:29 -0700

Surely there isn't -- says Rep. Rick Boucher (D-Va.) in his support for a consumer lawsuit seeking to confirm that users of Sonicblue's ReplayTV system have the lawful right to skip commercials when they record TV programs for later viewing. The suit has been filed in the same federal court in Los Angeles that is hearing a complaint from movie and television studios that ReplayTV allows customers to violate their copyrights, arguing that skipping commercials amounts to stealing. Sonicblue's position is:

"Basically we believe that consumers have 'fair-use' rights, and everything consumers do with a ReplayTV is covered with 'fair use'." [Reuters/*USA Today*, 6 Jun 2002, <http://www.usatoday.com>: NewsScan Daily, 7 June 2002]

⚡ **Dim STARS**

"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>

Fri, 07 Jun 2002 19:15:36 +0200

The US gave up on its Advanced Automation System (AAS) for air-traffic control in the mid-90's, for the "usual" reasons: large cost overruns and schedule slippages. The UK, however, whose 2MLoC [million lines of code] NERC system was approximately half (1MLoC) AAS code, decided to continue with development. The US instead went for a series of targeted solutions, starting with the Display Replacement System (DRS) for its en-route centers (those dealing with traffic en-route) in the late 90's, and continuing with new hardware for its HOST system, which drives the en-route displays. Among the major systems still under development is the Standard Terminal Automation Replacement System (STARS), which was to be installed at some 170+ (now 160+) locations, for departing and arriving traffic at TRACONS (Terminal Area Control facilities, controlling airspace around major airports), to replace the aged ARTS systems. A full list of FAA ATC systems under development may be found in [1].

STARS was contracted in 1996 to be delivered in 1998. The full software is now scheduled to be delivered in 2002. STARS is described as a "commercial off-the-shelf" (COTS) system (see [2]), quite the buzzword nowadays, and was the type of thing the US wanted to try instead of the "bespoke" AAS that was canceled in 1994. STARS was budgeted at \$940m, including installation costs at some 170+ TRACONS. John Mica, Chair of the House Aviation Subcommittee,

said in March 2001 [2] that the cancellation of the AAS "[cast] aside 11 years of development work and, according to GAO, [wasted] more than \$1.5 billion of taxpayer money."

This supposedly COTS system was restructured by the FAA and the supplier, Raytheon, into a "major redevelopment program" in 1998, because the COTS system "proved to be inadequate", being "[unable to] handle the high volumes of traffic required", with a corresponding \$1.4b price tag (Mica [2]). STARS is about 960 KLOC of core system i.e., that part of the software that is common to other STARS installations, such as in Germany and elsewhere (Marchilena, Executive VP of Raytheon, [2]) and about 400KLOC of "bespoke" code (Mead, DOT Inspector General, [2]).

In February 2002, Kenneth Mead, Inspector General of the US Department of Transportation, said that STARS "is already 4 years late and is now estimated to cost \$600 million over the original estimate of about \$1 billion. [...] Delays with STARS causes FAA to take stopgap measures for some facilities. FAA spent \$85 million to purchase and install Common ARTS systems [developed by Raytheon rivals Lockheed Martin Air Traffic Systems, formerly Loral, formerly IBM Federal Systems. PBL] at large facilities to replace aging equipment. FAA has spent about \$660 million on the STARS program but has only two Early Display Configuration systems in operation, which provide new controller displays, but rely on older software. The Early Display Configuration should not be confused with Full Service

STARS (Full STARS), which includes both new equipment and a complete replacement of older software." [1] Inspector General Mead has recently reported that STARS will cost at least \$1.7 billion, "an 80 percent increase over the initial estimate" [3]. Mead had testified before the Transportation Subcommittee of the House Appropriations Committee on March 13, 2002 that there were 258 open critical trouble reports for STARS, having grown from 171 in September 2001. The FAA indicated, however, that there were only 50 open critical trouble reports. Mead reviewed FAA documentation (the STARS Biweekly Report for March 7, 2002) and concluded that the figure of 258 was correct [3]. (A trouble report is open until closed, meaning a fix has been identified, documented, verified and validated. "Critical" open trouble reports are "those that would prevent or preclude the performance of a mission, jeopardize safety or security, or adversely affect a mission-essential capability." [3])

The FAA is aiming for the first installation of Full STARS at Philadelphia in November 2002. They are aiming for a product that is "not perfect, but acceptable", that is, to fix the "potential show-stoppers". As of May 2, there were 221 open critical trouble reports. The FAA now distinguishes between "critical" otr's and "truly critical" otr's. Mead calls the distinction "not self-defining and [...] vague" [3, p3].

Apparently, to stay on schedule for November 2002 deployment in Philadelphia,

the FAA has deferred independent testing. They were going to conduct the tests on Full STARS in Memphis in August 2002 to identify and correct glitches before installation in Philadelphia. But because of delays in development, Full STARS has not been installed in Memphis and independent testing will be performed after (!) Full STARS installation in Philadelphia [3].

Further, "in order to stay on schedule for Philadelphia, the contractor increased monthly spending (the "burn rate") in fiscal year 2002 to an unsustainable level [.....] [to] about \$10 million per month on average this year [...] an increase from a monthly average of \$8 million to \$9 million in the 3 prior fiscal years." [3]

Mead concludes "We have little doubt that STARS hardware and software can be "installed" by November, but, in our opinion, it is doubtful that it will be operationally suitable by November to control live air traffic in Philadelphia and replace ARTS." [3]

One might compare also the news reports by Bruce Nordwall in Aviation Week in March 2002 [4], and the AP brief in the International Herald Tribune on June 6, 2002 [5]. However, the IHT thinks that Mead said 71 open critical trouble reports, rather than the 258 that Mead says he said [3], and Nordwall says Mead said 175. Caveat lector.

References

[1] Status on the Federal Aviation Administration's Major Acquisitions, Memorandum from the DoT Inspector General, February 22, 2002.

http://www.oig.dot.gov/item_details.php?item=701

[2] Minutes of the House Aviation Subcommittee Meeting of March 14, 2001, at www.house.gov/transportation/aviation/03-14-01/03-14-01memo.html

[3] Follow-up Memo to FAA on STARS Acquisition, Memorandum from the DoT Inspector General, June 3, 2002. http://www.oig.dot.gov/item_details.php?item=806

[4] FAA Faulted for Slow Progress In ATC Modernization, Bruce D. Nordwall, Aviation Week and Space Technology, 18 March 2002, available to subscribers at www.awsonline.com

[5] New air traffic system under fire, Association Press, International Herald Tribune, Thursday June 6, 2002, available at www.iht.com

Peter B. Ladkin, University of Bielefeld
<http://www.rvs.uni-bielefeld.de>

✶ Questions about new air-traffic computer system

Ian Macky <ian.macky@oracle.com>
Wed, 5 Jun 2002 14:10:15 -0700 (PDT)

There are some highly scary quotes in this article regarding the new STARS (Standard Terminal Automation Replacement System) which is supposed to replace the hodge-podge of old air-traffic control systems:

<http://www.cnn.com/2002/TRAVEL/NEWS/06/05/faa.airtraffic.ap/index.html>

Players are the FAA Union (representing the flight controllers), the

FAA technicians who are trying to roll out the new system, the equipment builder, Raytheon Co., and the DOT (Department of Transportation). [...]

"DOT Inspector General Kenneth Mead ... said there were 71 specific software problems that could prevent the system from operating as designed, or could threaten safety or security. "

"Mead said controllers in El Paso had to track airplanes manually because the computer system didn't properly display the flights."

Union vice president Tom Brantley: "They don't believe it's operationally suitable," Brantley said. "It's failing. It has a lot of errors. They can't verify that it works because it fails a lot of the tests."

FAA spokesman Scott Brenner said the only problems are the normal bugs (!) that accompany any new technology. [Ship it!]

"When the [FAA] technicians refused to certify the system in Syracuse, New York, the FAA invoked a never-before-used [emergency] clause in its contract with its employees and ordered them to approve the equipment. The Syracuse system was turned on Monday night."

Brantley: "The emergency clause was never intended for something like this. That was intended if there were an actual emergency."

Blanche Necessary (!), a spokeswoman for the equipment builder, Raytheon Co., said the system was working well in El Paso and Syracuse.

etc., etc. The RISKS are painfully familiar.

Feel safer flying?

✈ COTS versus Bespoke ATC Systems

"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>

Fri, 07 Jun 2002 19:17:18 +0200

I have noticed that people talking about air-traffic control system software like to make a distinction between "commercial off-the-shelf" (COTS) systems, and bespoke systems (for example, [1]). I have long found this distinction unimportant in this domain, because of the amount of bespoke tailoring required for any ATC installation. But its usage seems to me to be increasingly prevalent. So I'd like to quantify my view with two examples.

The UK NERC system is an en-route system with 2MLoC software, which is about half common software (well, common with the now-defunct US AAS) and half bespoke. Development was budgeted at roughly GBP 500M (roughly \$750M) in the time frame 1992-1996. It finally came on-line in January 2002, with significant cost overruns. (How expensive the development effort really was depends on how one does the accounting. My estimates of 1998 turn out to have been fairly accurate. [2]) Schedule slippage was 6 years on 4 years planned.

The US STARS system was bought as a "COTS" system. STARS has undergone \$660m of development work to date and a schedule slippage of 4 years

(to an original schedule of 2 years until first installation in 1998), and is about two thirds code in common with other installations (e.g. in Germany), that is, 960 KLOC, and one third bespoke, 400+ KLOC. Full STARS software is thus two thirds as large as NERC software. Development has cost \$660 million so far, for a November 2002 first (full) deployment.

So the difference between "COTS" and "bespoke" appears to be one-sixth (the difference between two thirds and one half), and buying "COTS" systems does not necessarily save one from comparable cost overruns or schedule slippages. The LOC count for STARS is about two thirds that for the NERC software; the development costs to first deployment seem also to be comparable (NERC has only one installation, compared with STARS's planned 160+, so total program costs for STARS are higher than for NERC). And schedule slippages are roughly the same magnitude (if strict proportionality is your thing, total:planned time yields 9:4 for NERC and 6:2 for STARS).

I conclude that "COTS" and "bespoke" is not a helpful predictive distinction for ease and comparative cost of development and deployment of ATC systems.

References

[1] Minutes of the House Aviation Subcommittee Meeting of March 14, 2001, at www.house.gov/transportation/aviation/03-14-01/03-14-01memo.html

[2] Memorandum to the Transport Sub-Committee on the Costing of NERC, 26

November 1998, Memorandum FN 12 in (UK) House of Commons,
Session 1998-99,
Environment, Transport and Regional Affairs Committee, Third
Report, The
Future of National Air Traffic Services, pp52-55. Also available
as
RVS-S-98-02 of 26 November 1998, at www.rvs.uni-bielefeld.de ->
Publications
-> Special Reports

Peter B. Ladkin, University of Bielefeld
<http://www.rvs.uni-bielefeld.de>

✉ **Re: Swanwick (Brady, [RISKS-22.09](#))**

"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>
Fri, 07 Jun 2002 19:16:26 +0200

Chris Brady notes that the UK's New En-Route Center (NERC) at
Swanwick, which
came on-line in January 2002, crashed "yet again" on May 17th.

Well, it did, but that's the first time, to my knowledge. Other
recent
outages, including one on March 27 in which I was caught,
reported in
[RISKS-21.98](#) by Alistair Macdonald and Simon Waters, involved the
National
Airspace System (NAS) in West Drayton, which processes flight
plan data
which is fed to the NERC (Martyn Thomas, [RISKS-22.02](#)). When this
data is
generated and manipulated by hand, as during a NAS failure, many
fewer
aircraft are allowed into the system.

The NERC is an airspace management aid. It is essentially a
display system

for data which comes from other systems (radar feeds, NAS, and so forth). The worst kind of outage is one in which the system fails in use. As far as I know, this has not happened. The BBC reported that engineers failed to bring the system fully back up after a system upgrade. A number of controller workstations were inoperative (<http://news.bbc.co.uk> and search for "Swanwick") and service was restored fairly quickly (a matter of hours). As failures go, that is technically relatively benign, and completely benign as concerns safety. Of course, one would prefer not to have any.

Brady says that the upgrade rendered "half the air traffic controllers' computer screens inoperable". The BBC reported that six out of twenty displays did not come up.

Brady wonders how much all this outage is costing the airlines. The answer is: more than one might think, for the airlines also own and manage NATS.

In a second note concerning difficulties some controllers are having in reading data on the screens at the NERC, Brady says "Obviously no-one thought to ask the controllers if they could actually read the screens clearly".

On the contrary, controllers were evaluating and training on the system for at least two years before it went live in January, and it is public knowledge that they were very active with their feedback. NATS recognised in 1998 the need for a transition period more extended than the

originally
planned six months (I suspect they knew it well before that, but
there would
have been constraints on their replanning).

Brady says that the NERC is "a disaster waiting to happen". It
is unclear to
me how he reaches this conclusion. He seems to think that one
outage
portends disaster. The record could equally well be taken as
evidence for a
well-managed and well-functioning system: one glitch in a system
build in
four months, and no live crashes. Reader's choice (along with
any position
in between).

That all said, it is appropriate to wonder, as Brady does, why
there is now
a cluster of system slowdowns and outages, after years of
successful NATS
systems operation, including times when various systems have
been strained
to and even over what was thought to be their capacity and have
proved much
more resilient than most people had imagined. John Stuart Mill's
Method of
Differences would lead us to look for causal factors around what
has
recently changed, and the most obvious recent large change is the
introduction of the NERC in January into the live airspace
management
system. In so far as there is a risk obvious to everybody, that
was it. The
management of this change will have affected other subsystems of
the
national airspace management, including NAS of course.

One should not underestimate the technical challenge involved in
switching
to this new system. ATC systems are built in an environment in
which
requirements constantly change; they are safety-related and hard-

real-time;
and every one has components adapted from other systems and
components
unique to itself. All the system-engineering bad apples in one
basket,
except one: ATC system design has traditionally employed "graceful
degradation" in the guise of a radio-only reversion mode (which
will
sometime no longer pertain when traffic is allowed to become
sufficiently
dense, whereupon the ATC system will become safety-critical
rather than
safety-related). The airspace NERC covers includes some of the
busiest in
the world, and it is to my knowledge the largest live ATC system
anywhere
(2MLoC), though not the most expensive (that honor belongs to
the deployment
of STARS in the US, as far as I know). I imagine management of
this
enterprise has been learning by doing. And unavoidably so.

For what it's worth, the NERC is a system Brits made work after
America gave
up. In the last few years, I have found myself puckishly drawn
to two
images. One is Dr. Johnson's "... dog walking upon his hind
legs. It is not
done well; but you are surprised to find it done at all." The
other is that
of old American cars in Cuba (the NERC uses a token ring
architecture, after
all). However, the US got its replacement systems (the 1.3 MLoC
STARS, inter
alia) no more quickly, by no means less expensively, and
apparently with no
less trouble (see [1] and [2]). Again, reader's choice.

References

[1] Dim STARS, Peter B. Ladkin, 7 June 2002. [[RISKS-22.12](#)]

[2] COTS versus bespoke ATC systems, Peter B. Ladkin, 7 June

2002.

[[RISKS-22.12](#)]

Peter B. Ladkin, University of Bielefeld, Germany

<http://www.rvs.uni-bielefeld.de>

[Incidentally, Nancy Leveson reports that she was told STARS has 5MLoC, although that may represent different code boundaries from the smaller numbers. PGN]

✶ COTS versus Bespoke ATC Systems (Re: Ladkin, [RISKS-22.12](#))

Nancy Leveson <leveson@sunnyday.mit.edu>

Fri, 07 Jun 2002 14:16:12 -0400

> NERC has only one installation, compared with STARS's planned 160+

This is an important point... In the U.S., every ATC facility does things differently, often significantly differently. The problem of trying to develop and install 160 different systems with each different than the others is orders of magnitude more difficult from both a software engineering and installation standpoint.

I was involved with a software tool that simply assisted TRACON controllers with arrival traffic. That software (about 500 KLOC of C code) contained 50,000 KLOC of what was called "adaptation data" that was needed for the Dallas/Ft. Worth installation with which I was involved. The experimental software was designed originally for DFW, with the intention of

changing the
adaptation data for other TRACON facilities. That has proven to
be more
difficult (and expensive!) than expected.

***NY Times* new-zero security password system**

Martin Ward <Martin.Ward@durham.ac.uk>

Wed, 5 Jun 2002 11:33:05 +0100 (BST)

The New York Times has recently switched their paid user
accounts from a
reportedly hard to use and unreliable password system called
Qpass to a new
system. They then sent an e-mail message to all account holders:

Now enter the following Member ID and password which we have
created

for you and click the "Log In" button. You will need to use
this

Member ID and Password to access your NYTimes.com premium
products
in the future.

Member ID: ZZZZ

Password: Your password is your Qpass User Name.

The member id (ZZZZ above) is in the form `firstname_lastname` and
Qpass user
names are easily guessable, often repeated across many sites,
and often not
kept as secrets (for instance, message board posts are often
tagged by
username).

The New York Times response to complaints about this system
was that you
could always change your password if you found yourself
concerned about

security.

See <http://www.oreillynet.com/cs/weblog/view/wlg/1482> for the full story.

Martin.Ward@durham.ac.uk <http://www.cse.dmu.ac.uk/~mward/> Erdos number: 4

[An item by Marc Hedlund on this problem was noted by Peter Tonoli:

http://www.nytimes.com/ref/membercenter/help/gpass_redir.html
PGN]

✶ Tracking subway users by electronic fare card

Ngiam Shih Tung <stngiam@pobox.com>

Tue, 28 May 2002 22:01:19 +0800

The New York Times (2 Apr 2002) recently reported that investigators trying to determine how a New York woman had contracted Anthrax during last year's bioterrorist attack had used subway computer records and her fare card to trace her movements in the city prior to her death.

Admittedly, the victim was dead and privacy rights are generally recognised to be extinguished on death, but if a dead person's subway rides can be tracked, so can a live person's.

Does anyone know what is the legal position on fare card records in New York and elsewhere ? Is there any legal barrier or policy that would prevent a transit authority from releasing fare card records to any law enforcement agency, or to anyone ?

None of the media reports mentioned how far back in time the investigators were able to trace Nguyen's movements. Can anyone hazard a guess on how long New York's MTA keeps fare card data ?

✶ Kazaa users inadvertently share their private files

Nathan Good <ngood@exch.hpl.hp.com>

Wed, 5 Jun 2002 17:10:02 -0700

We have just finished a study that shows how user interface design flaws allow users on Kazaa to share their personal files without their knowledge. In a laboratory user study, only 2 out of 12 subjects were able to correctly determine that Kazaa was sharing their entire hard drive. We looked at the current Kazaa network and discovered that many users are sharing personal information such as email and data for financial programs such as Microsoft Money.

To see if other users on Kazaa were aware of this and taking advantage of users ignorance, we ran a Kazaa client for 24 hours with dummy personal files. During this time, files named "Inbox.dbx" and "Credit Cards.xls" where downloaded from our client by several unique users.

The tech report can be accessed here:

<http://www.hpl.hp.com/shl/papers/kazaa/KazaaUsability.pdf>

or from our lab web page at

<http://www.hpl.hp.com/shl/>

Nathan Good, Information Dynamics Lab, HP Laboratories ngood

@hpl.hp.com

1501 Page Mill Road, Palo Alto, CA 94306, USA 1-650-236-4437

✦ Web glitch exposed Fidelity accounts

Monty Solomon <monty@roscom.com>

Mon, 3 Jun 2002 01:57:08 -0400

Canadian account holders information was accessible, AP, 29 May 2002

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.

<http://www.msnbc.com/news/758979.asp>

✦ Hacker threat posed by Excel spreadsheets

"Patrick O'Beirne" <yg02@sysmod.com>

Wed, 29 May 2002 15:56:36 +0100

<http://www.silicon.com/a53624>

Tuesday 28th May 2002 11:20am

A security hole in Excel XP spreadsheets which could lead to a hack attack

has been exposed. The discovery was made by independent security expert Georgi Guninski, who said on his Web site: "Excel XP tries to play with new technologies like XML and XSLT. Unfortunately the Excel seem so flawed that if the user opens a .xls file and chooses to view it with xml stylesheet arbitrary code may be executed. As script kiddies know this may lead to taking full control over a user's computer." Guninski, who has posted a sample of the code in his site, said users should not use XML stylesheets.

⚡ Re: More on typos and homographs ([RISKS-22.11](#))

Martin Wheatman <martin.wheatman@hp.com>

Fri, 7 Jun 2002 09:44:20 +0100

I have been informed by Malcolm Pack that I was wrong about the protection of the .co.uk domain, which involves no checks whatsoever. The protected ones with stringent requirements are .ltd.uk and .plc.uk (which are private and publicly listed companies in the UK) and .sch.uk for schools and .ac.uk for academic institutions. <<http://www.nic.uk/rules/rup1.html>>

[This message is a combination of Martin's and Malcolm's items. PGN-ed]

⚡ Re: More on typos and homographs (Wheatman, [RISKS-22.11](#))

Scott Nicol <snicol@apk.net>

Thu, 06 Jun 2002 22:04:38 -0400

Are you sure [about llyodstsb.com]? You may want to change your password:

whois llyodstsb.com gives

Registrant:

Lloyds Bank Plc (LLOYDSTSB2-DOM)
Network Services
64 Hopton Street, London SE1 9JQ
United Kingdom

whois llyodstsb.com gives

Registrant Contact:

FastNet Corporation
Kwai Wei Suh (fastnet22@yahoo.com.hk)
852-4326-7127
339 Huan Shi Dong Road
Guangzhou, AL 510098
CN



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 13

Thursday 27 June 2002

Contents

- [Secret American spy photos broadcast unencrypted over satellite TV](#)
[Duncan Campbell via Tim Finin via Dave Farber](#)
- [Software problem kills soldiers in training incident](#)
[Steve Bellovin](#)
- [Safety and human factors in ATC](#)
[via Hayley Davison and Nancy Leveson](#)
- [Car repair shops often can't crack diagnostic code](#)
[Monty Solomon](#)
- [Qui audit ipsos auditors?](#)
[Rob Slade](#)
- [Tools gauging blood pressure raise questions](#)
[Monty Solomon](#)
- [Microsoft's secret plan to secure the PC](#)
[Monty Solomon](#)
- [Risks to your privacy from using MSN Messenger 4.6?](#)
[Michael Weiner](#)
- [Microsoft sent Nimda worm to developers](#)
[Mike Hogsett](#)
- [Microsoft's Allchin: API disclosure may endanger U.S.](#)
[Brien Webb](#)

- [Identity theft site](#)
[Conrad Heiney](#)
 - [Randomly generated 4-letter words in sendmail queue-ids](#)
[Earle Ake](#)
 - [New virus can infect picture files](#)
[NewsScan](#)
 - [Norwegian history database password lost and retrieved](#)
[Lillie Coney](#)
 - [Calculators vs. handheld computers](#)
[NewsScan](#)
 - [England halts distribution of bad money](#)
[Monty Solomon](#)
 - [E-mail address parsing](#)
[William Colburn](#)
 - [Risks subscription problem](#)
[Ethan Benatan](#)
 - [Re: NERC + token ring](#)
[T Panton](#)
 - [Re: US Navy suffers domain hijacking](#)
[Jay R. Ashworth](#)
 - [Re: Please ignore the anti-shoplifting device!](#)
[Scott Peterson](#)
 - [REVIEW: "Developing Trust", Matt Curtin](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ Secret American spy photos broadcast unencrypted over satellite TV

Dave Farber <dave@farber.net>
Thu, 13 Jun 2002 22:39:31 +0900

[from Tim Finin, Prof Computer Science & Electrical Eng,
Director Inst. for
Global Electronic Commerce, U Maryland Baltimore County, 1000

Hilltop,

Baltimore MD 21250 finin@umbc.edu 410-455-3522 <http://umbc.edu/~finin/>

Dave's IP archives at:

<http://www.interesting-people.org/archives/interesting-people/>]

Now showing on satellite TV: secret American spy photos;

Security lapse allows viewers to see sensitive operations
Duncan Campbell, Thursday June 13, 2002, *The Guardian*

European satellite TV viewers can watch live broadcasts of peacekeeping and anti-terrorist operations being conducted by US spyplanes over the Balkans.

Normally secret video links from the American spies-in-the-sky have a

serious security problem - a problem that makes it easier for terrorists to

tune in to live video of US intelligence activity than to get Disney

cartoons or new-release movies. For more than six months live pictures from

manned spy aircraft and drones have been broadcast through a satellite over

Brazil. The satellite, Telstar 11, is a commercial TV relay. The US

spyplane broadcasts are not encrypted, meaning that anyone in the region

with a normal satellite TV receiver can watch surveillance operations as

they happen. The satellite feeds have also been connected to the Internet,

potentially allowing the missions to be watched from around the globe.

<http://www.guardian.co.uk/international/story/0,3604,736462,00.html>

Software problem kills soldiers in training incident

Steve Bellovin <smb@research.att.com>

Thu, 13 Jun 2002 09:38:10 -0400

According to a U.S. Army report, a software problem contributed to the deaths of two soldiers in a training accident at Fort Drum. They were firing artillery shells, and were relying on the output of the Advanced Field Artillery Tactical Data System. But if you forget to enter the target's altitude, the system assumes a default of 0. (A Web site I found indicates that (part of) Ft. Drum is at 679 feet above sea level.) The report goes on to warn that soldiers should not depend exclusively on this one system, and should use other computers or manual calculations.

Other factors in the incident include the state of training of some of the personnel doing the firing. [Source: AP]

Steve Bellovin, <http://www.research.att.com/~smb> (me)
<http://www.wilyhacker.com> ("Firewalls" book)

✶ Safety and human factors in ATC (via Hayley Davison and Nancy Leveson)

Peter Neumann <neumann@csl.sri.com>

Fri, 14 Jun 2002 11:03:25 -0400

Air control safety complaints soar
By Paul Marston Transport Correspondent
Daily Telegraph (Britain), 14 Jun 2002 [PGN-ed]

The number of formal complaints of over-work from air-traffic controllers has more than doubled since the Swanwick national control centre opened in January 2002. National Air Traffic Services (NATS) said staff had filed 30 "overload" reports in the last five months, compared with 12 during the same period in 2001. [Computer-related problems related to Swanwick and UK ATC are noted in [RISKS-22.02,03,09,12.](#)] Planning staff at Swanwick have also complained about the legibility of some flight levels and airport codes on their terminal displays.

✈ Car repair shops often can't crack diagnostic code

Monty Solomon <monty@roscom.com>

Tue, 25 Jun 2002 01:32:16 -0400

At least a couple of times a week, mechanic Ernie Pride tells customers at his independent repair shop he can't fix their cars because he doesn't know what's wrong with them. Go to the dealer, he advises. He has the experience and knowledge to service vehicles but lacks the closely guarded information needed to diagnose problems with today's high-tech cars. Automakers refuse to make much of it available to independent shops that compete with higher-priced dealerships. The practice is raising hackles in Congress and a vigorous defense by the industry. ... [AP, June 24, 2002]
<http://www.cnn.com/2002/TECH/ptech/06/24/diagnosing.cars.ap/>

✶ Qui audit ipsos auditors?

Rob Slade <rslade@sprint.ca>

Wed, 19 Jun 2002 14:25:37 -0800

The Enron/Anderson debacle is fading as news, but it has some reverberations for those of us in the info tech fields.

Anderson is not alone in engaging in questionable audit practices. Others of the "Big 5" are under scrutiny, in at least two cases involving, ironically, high tech companies. For the past decade or more, there have been pressures to reduce regulatory oversight, and we are now seeing the results.

So, what is the relation to IT? Well, these are the same firms who hold the major contracts for auditing information security and assurance.

(In relation to the subject line: yes, "ISACA," I know.)

rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

<http://victoria.tc.ca/techrev> or <http://sun.soci.niu.edu/~rslade>

✶ Tools gauging blood pressure raise questions

Monty Solomon <monty@roscom.com>

Fri, 21 Jun 2002 23:00:04 -0400

Gina Kolata, *The New York Times*, 16 Jun 2002

Across the nation, hospitals and doctors' offices are returning blood pressure cuffs to their manufacturers to comply with a federal environmental initiative to cut down on the use of mercury, a toxic metal that can pollute the air and water when disposed of improperly. But leading medical experts, joined by the American Heart Association and the National Heart, Lung and Blood Institute, say the mercury gauges are being replaced by newer devices that may be unreliable, and they warn that inaccuracies may be leading to false diagnoses and inappropriate treatments. [...]
<http://www.nytimes.com/2002/06/16/health/16BL00.html>

Microsoft's secret plan to secure the PC

Monty Solomon <monty@roscom.com>
Tue, 25 Jun 2002 01:40:54 -0400

You've heard of Trustworthy Computing, and the massive corporate remodeling going on at Microsoft where every developer, product manager, and executive assistant has been asked to rethink everything they do in the context of security. Well, that's just the tip of the iceberg. Secretly, the company has been working on a plan to rearchitect the PC from the ground up, to address the security, privacy, and intellectual property theft issues that

dog the industry today. Inexplicably, the company pulled an Apple and chose to detail its plans solely to Newsweek, so we only have that one report to work from. But if Newsweek's take on the plan is correct, and consumers and businesses buy into the new devices that would result, the PC landscape will soon change forever. [...]

<http://www.ntsecurity.net/Articles/Print.cfm?ArticleID=25681>

⚡ Risks to your privacy from using MSN Messenger 4.6?

"Michael Weiner" <michael_weiner@gmx.net>

Tue, 18 Jun 2002 17:44:11 +0200

Since I installed MS Messenger 4.6 (4.6.0082) on my machine, my firewall is going wild: In addition to numerous Microsoft sites, Messenger is contacting the following sites each time I log in: expedia.com, xp.mcafee.com, carpoint.msn.com and port-64-1956779-zzt0prespect.devices.datareturn.net. No way to know what information MS Messenger is transmitting to these sites, I did not find any meaningful information on it on the Microsoft website...

⚡ Microsoft sent Nimda worm to developers

Mike Hogsett <hogsett@csl.sri.com>

Fri, 14 Jun 2002 17:26:34 -0700

Microsoft accidentally sent the virulent Nimda worm to South Korean developers when it distributed Korean-language versions of Visual Studio .Net that carried the virus, the company acknowledged Friday.

<http://news.com.com/2100-1001-935994.html>

Microsoft's Allchin: API disclosure may endanger U.S.

Active Quality Software <activequalitysw@la.com>

Fri, 14 Jun 2002 12:09:43 -0700

>From a 2002/05/13 article by Caron Carlson in eweek.com:

<http://www.eweek.com/article/0,3658,s%253D701%2526a%253D26875,00.asp>

"A senior Microsoft Corp. executive [Jim Allchin] told a federal court last week that sharing information with competitors could damage national security and even threaten the U.S. war effort in Afghanistan. He later acknowledged that some Microsoft code was so flawed it could not be safely disclosed."

and later, directly quoting Allchin...

"Computers, including many running Windows operating systems, are used throughout the United States Department of Defense and by the armed forces of the United States in Afghanistan and elsewhere."

Microsoft proposes to withhold details of the MSMQ protocol (TCP port 1801

and UDP port 3527), the Windows File Protection API, as well as APIs for anti-piracy protection and digital rights management under the security carve-out.

I recall that the Windows NT family of operating systems was designed to meet DOD's C2 security criteria, including the Orange Book (standalone, which they passed), as well as Red Book (networking) and Blue Book (subsystems) criteria which they started working on at least 4 years ago; I don't know if they've yet passed, but I suspect not if it's so flawed that they don't want to disclose the protocol or API! See <http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnproasp2/html/windowsntsecuritysystems.asp>

So, one risk of flawed software might be that you have to publicly invoke national security (read patriotism) as a last refuge from legal process.

--Brien Webb <http://www.LA.com/>

Identity theft site

"Conrad Heiney" <conrad@fringehead.org>

Wed, 26 Jun 2002 15:32:48 -0700

According to CNN's website today

<http://www.cnn.com/2002/TECH/internet/06/26/identity.theft.ap/index.html>

a nongovernmental organization called CardCops is providing a service in which consumers can check to see if their credit cards have been

abused in
some way.

The check is done by visiting the website and entering your
credit card
number.

The RISKS here are bad enough to be humorous. Although CardCops
themselves
appear to be a legitimate organization (at least at time of
press) , and do
not themselves ask for the expiration date required to complete a
transaction, there's no protection against copycat websites
whose intent is
entirely evil, or telephone scams based on the CardCops
publicity. The
quality of the data is another obvious minefield.

[And as of today, their site is also down due to high volume.]

Conrad Heiney conrad@fringehead.org <http://fringehead.org>

✶ Randomly generated 4-letter words in sendmail queue-ids

Earle Ake <earle.ake@hcst.com>

Mon, 17 Jun 2002 16:59:38 -0400 (EDT)

I was checking the sendmail queue today when I noticed a message
with a
certain 4-letter word as part of the queue id that ends in
"uck". I checked
the sendmail logs further and there was another 4 letter word as
part of
another queue id that also ends in "uck" and another that ends
in "ock" with
a certain letter before it. I wonder how many people pay
attention to queue
IDs and would raise an eyebrow on those. I also wonder if any

of the filtering software out there might filter out legit mail messages just because certain random 4 letter words were contained in the queue-id that are inserted into the mail headers as they pass through each system.

✶ New virus can infect picture files

"NewsScan" <newsscan@newsscan.com>

Fri, 14 Jun 2002 08:32:37 -0700

McAfee Security is reporting that a new virus called "Perrun" is the first ever to infect picture files, which, along with other data files, have long been considered safe from such threats. Researchers at McAfee received the virus from its creator and say it's what's called a proof-of-concept virus and does not cause any damage. Up until now, viruses infected and were spread through program files; data files might be deleted or damaged, but Perrun is the first to infect them by inserting portions of the virus code into the picture file. When a .JPG picture is viewed, the virus installs a file on the victim's hard drive that can infect other pictures. Because the original picture looks fine, the victim won't know that anything's amiss.

[AP, 13 Jun 2002; NewsScan Daily, 14 June 2002]

<http://apnews.excite.com/article/20020613/D7K4F4EG1.html>

⚡ Norwegian history database password lost and retrieved

Lillie Coney <lillie.coney@acm.org>

Tue, 11 Jun 2002 11:37:02 -0400

After the password for accessing a Norwegian history museum's database catalog for 11,000 books and manuscripts had been lost when the database's steward died, the museum established a competition to recover it. Joachim Eriksson, a Swedish game company programmer, won the race to discover the password (ladepujd, the reverse of the name of the researcher who had created the database). How he arrived at it was not disclosed.

[Source:

Long-lost password discovered: Norwegian history database cracked with help from the Web, By Robert Lemos, MSNBC, 11 Jun 2002; PGN-ed]

Lillie Coney, Public Policy Coordinator, U.S. Association for Computing

Machinery Suite 510 2120 L Street, NW Washington, D.C. 20037 1-202-478-6124

⚡ Calculators vs. handheld computers

"NewsScan" <newsscan@newsscan.com>

Wed, 12 Jun 2002 08:01:42 -0700

As handheld computers become increasingly competitive with Texas Instrument (TI) calculators for mathematical graphing, TI has been busy adding features such as address books, organizers, and a large variety of spreadsheet

programs. The main advantage of handhelds, of course, is that they are general-purpose devices. Nelson Heller, who publishes the Heller Report newsletter on education technology, says that both calculators and handheld computers are getting better but adds: "The question I see is whether a specialized appliance like the graphing calculator will in the long run lose out to a more generalized appliance like a PDA." Calculators, however, still have two advantages: lower cost (about half of a PDA's cost) and acceptability in testing situations, in that students are permitted to use calculators but not handheld computers when taking the Scholastic Aptitude Test. The reason? Fear that some students might use the infrared messaging capability of handhelds to cheat on the test. (AP/*San Jose Mercury-News*, 12 Jun 2002; NewsScan Daily, 12 June 2002)

<http://www.siliconvalley.com/mld/siliconvalley/3453135.htm>

[And exam proctors will be able to determine that the so-called "calculator" is not surreptitiously a general-purpose device? PGN]

✶ England halts distribution of bad money

"monty solomon" <monty@roscom.com>

Tue, 28 May 2002 13:01:11 -0400

The Bank of England asked banks Monday to stop issuing its new anti-counterfeit 5-pound notes after discovering that serial numbers on the currency could be rubbed off. [AP, 27 May 2002]

<http://news.lycos.com/news/story.asp?>

[section=World&storyId=423067](#)

✶ E-mail address parsing

"Schlake (William Colburn)" <"@ @"@nmt.edu>

Fri, 21 Jun 2002 14:23:45 -0600

About the same time PGN posted to the list about RISKS SPAM, I got a call from someone who was going through corporate-education on e-mail addresses. She had been given a test, and she had to identify which e-mail addresses were valid. She was told that half of them were invalid. The purpose of the test was to train employees to be able to properly harvest the e-mail addresses of their elderly customers. As far as I can tell, all of them were valid.

The very next day, I made myself a new e-mail address, "@ @"@nmt.edu. I like this address, it has been a lot of fun so far. No customer-relations software seems able to accept that this is a valid e-mail address. People seem pretty trusting, and are willing to try and (and are surprised when it works).

The risk is that the customer-relations programmers are living in a world of [a-z0-9_] for mailbox names, while the standard has long allowed for virtually any character (including NULL). More and more services are unavailable if you "don't have an e-mail address", and usually even the web form to submit a bug won't process because

it wants
your e-mail address, so they never even know. Even if I wasn't
taunting
them with "@ @", I'd be giving out my address with a "+" and
then the
name of their company to help me sort out where my SPAM is
really coming
from. Few pieces of software will allow even the harmless
little "+"
character in an address.

✶ Risks subscription

Ethan Benatan <ethan.benatan@reed.edu>
Thu, 13 Jun 2002 16:32:40 -0700

[In attempting to confirm a subscription request, Ethan's mail
system
responded to RISKS and not to majordomo. This seems to happen
from other
e-mail systems as well. PGN]

Eudora's recent MacOS X version is broken and ignores reply-to
headers;
older versions didn't used to do that.

✶ Re: NERC + token ring (Ladkin, [RISKS-22.12](#))

<tpanton@attglobal.net>
Tue, 11 Jun 2002 17:06:14 +0000 (GMT)

In [RISKS-22.12](#), Peter Ladkin mentions NERC's use of a token ring
as if this
were obviously a bad thing. If I remember correctly, a token

ring has better behaviour at high load (as compared to ethernet), because it implements a round-robin allocation and thus does not waste capacity in collisions.

Indeed a precursor (the Cambridge ring) had the endearing characteristic that high loads made the PLL clock drift fast, upping the capacity by a few percent. The risk is in assuming the dominant technology is best for all situations. URL: <http://www.westpoint.ltd.uk/> - Internet recon.

✶ Re: US Navy suffers domain hijacking (Brent, [RISKS-22.10](#))

"Jay R. Ashworth" <jra@baylink.com>

Tue, 11 Jun 2002 12:46:25 -0400

Thank you, Geoffrey, for you've given me a hook on which to hang one of my *favorite* rants.

"navydallas.com" (the proper spelling, for the DNS is case-insensitive by design) is *not* a "trusted domain", in any remote sense of the word. Nor is "myflorida.com" (an alias for www.state.fl.us, which apparently is too complicated for people) or "largo.com".

I have a *real* dislike for municipal and government web teams who have *so* little faith in their audience's mentalities that they feel they have to spurn the TLDs in which they *would* be protected -- and could be trusted

(the ".gov" and ".us" domains which have -- or perhaps in the latter case "had" -- restrictions on registration) -- for ".com", just because "that's the only thing people understand". <sigh>

At least it turned around and bit Largo Florida in the ass about a year ago when their mail server melted down under the load of 60K+ *bounce* and complaint messages when someone used "largo.com" as a forged return address on some spam.

I've seriously thought about registering "yourflorida.com" and putting up a website that looks very much like myflorida.com, but is parody (when you look closely enough), and which explains exactly why I think they are doing wrong... but while that wouldn't even *be* civil disobedience, much less copyright infringement (based on the Skyywalker Music case), the fact that no less a legal luminary than Lawrence Lessig thinks that civil disobedience is no longer a useful approach <http://www.reason.com/0206/fe.jw.cyberspaces.shtml> scares me to death.

Jay R. Ashworth, Baylink, Member of the Technical Staff, The Suncoast Freenet
Tampa Bay, Florida +1 727 647 1274 <http://baylink.pitas.com>
jra@baylink.com

✶ Re: Please ignore the anti-shoplifting device! (Hendricks, [R-22.12](#))

Scott Peterson <scott4@mindspring.com>

Thu, 06 Jun 2002 19:21:10 -0700

> I also realized that the alarm would likely sound as I exited
at the other
> end of the store.

Which also points out a whole series of other problems. I
worked with
corporate security for a large supermarket chain in So. Calif.
several
years ago.

I don't think the law has significantly changed, but at the
time, you, as
an individual, could not stop someone for a misdemeanor (like
shoplifting)
unless you saw them take the item and followed them until they
exited. If
you did, it was quite possible for you to be charged with
unlawful
detention getting both yourself and the company in big trouble.
Having an
alarm go off as you walk through it was not a good enough reason
to stop
someone. Only a sworn peace officer could stop someone in those
circumstances.

For this reason and the safety of the employees, they were
required to know
the store policy and follow it. If they suspected someone of
shoplifting
they were to call someone in management and let them deal with
it. Under no
circumstances were they to take any action on their own.

Bottom line: Those alarm units are often more a psychological
barrier than a
legal one.

REVIEW: "Developing Trust", Matt Curtin>

Rob Slade <rslade@sprint.ca>

Mon, 17 Jun 2002 08:00:56 -0800

BKDEVTRS.RVW 20020514

"Developing Trust", Matt Curtin, 2002, 1-893115-72-0, U\$39.95

%A Matt Curtin cmcurtin@interhack.net

%C 175 Fifth Ave., New York, NY 10010

%D 2002

%G 1-893115-72-0

%I Springer-Verlag/Apress

%O U\$39.95 212-460-1500 800-777-4643 orders@springer-ny.com

%P 282 p.

%T "Developing Trust: Online Privacy and Security"

The title, foreword, preface, and introduction aren't terribly clear

about the purpose of the book. Ultimately, the key word seems to be

not trust, but privacy: the work appears to be directed at providing

tips for developers, of all stripes, to help maintain the confidentiality of information.

Part one is a generic introduction to security and privacy.

Chapter

one, entitled "Why Privacy," seems, ironically, to move us even further away from the topic of privacy. The emphasis of the chapter

is on intrusions, although the reconnaissance phase does get the most

space. (The subtitle, "Why This Book," does not appear to be addressed.) The discussion of privacy theory, in chapter two, flips

back and forth between the technical issues of identity authentication

and access control, and the social concepts of privacy, failing to

make hard relations between the two ideas. A partial list of basic

conceptual security terms are reasonably well defined in chapter three. Chapter four does start to get into privacy issues, specifying a number of notions important to protecting confidentiality in an online (generally Web based) environment. A number (but not an exhaustive list) of threats to privacy are discussed in chapter five.

Part two looks at the problem. Chapter six provides a concise list of the basic principles of development of secure applications. (Interestingly, Curtin uses the principle of least common mechanism as an argument for the adoption of modular code, where others might say that it was a reason to avoid modularity.) Background concepts for the Internet and Web, the basic development environment assumed for the book, are given in chapter seven. Some specific examples of privacy problems on the Web are presented in chapter eight.

Part three outlines the cure. Chapter nine reviews some basic security protections, such as firewalls and constrained systems. Opt out systems are criticized in chapter ten. "Earning Trust," in chapter eleven, points out that providing privacy for customers is not just a cost and a nuisance, but good business. A structure for analyzing and designing secure Web systems is proposed in chapter twelve.

Strangely, while the book is disjointed and difficult to pin down as to the central theme, ultimately it could be quite valuable. In the end, the title is appropriate, albeit in a punning fashion: the content is directed at developing trustworthy applications. The literature in the field of developing secure applications is not extensive, and much of it is either ethereally academic or completely language specific. This book attempts to be practical, and, while

hardly ever touching on implementation, the precepts suggested are a sound foundation. Security professionals would find the general background limited, but developers will neither be snowed under by esoteric discussions nor left with too many vulnerabilities uncovered. The specifics in the book deal with the Web, but the tenets of secure design are applicable to all systems.

copyright Robert M. Slade, 2002 BKDEVTRS.RVW 20020514
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

<http://victoria.tc.ca/techrev> or <http://sun.soci.niu.edu/~rslade>



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

[ACM](#) Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 14

Tuesday 9 July 2002

Contents

- [DCS/SCADA Security](#)
[Eytan Adar](#)
- [Fishermen rescued after dam malfunction](#)
[Thomas Dzubin](#)
- [China bans toxic American computer junk](#)
[Mich Kabay](#)
- [A Microsoft Medley in RISKS-22.13](#)
[Peter da Silva](#)
- [Windows Media Player security update EULA gives MS permission to keep you from using "other software" on your computer](#)
[Bill Tolle](#)
- [Re: E-mail address parsing](#)
[George Roussos](#)
- [MI5 hates encryption so much, they don't use it!](#)
[Ben Laurie](#)
- [More on The Telecom Crash of 2002](#)
[Joe Pistrutto via Dave Farber](#)
- [Security in General - wireless - simplicity](#)
[M Simon](#)
- [FORTH](#)

[M Simon](#)

● [11th USENIX Security Symposium](#)

[Alex Walker](#)

● [REVIEW: "Decrypted Secrets", F. L. Bauer](#)

[Rob Slade](#)

● [Info on RISKS \(comp.risks\)](#)

⚡ **DCS/SCADA Security**

Eytan Adar <eytanadar@yahoo.com>

Thu, 27 Jun 2002 09:33:59 -0700 (PDT)

>From an article about security of various control systems
(dams, trains,
etc.). My favorite quote from this article:

"Most of these devices are now being connected to the
Internet. But
because the digital controls were not designed with public
access in mind,
they typically lack even rudimentary security, with fewer
safeguards that
accompany the purchase of flowers online."

(this and other good stuff at:

<http://www.siliconvalley.com/mld/siliconvalley/3554402.htm>)

⚡ **Fishermen rescued after dam malfunction**

Thomas Dzubin <dzubint@vcn.bc.ca>

Fri, 28 Jun 2002 15:29:19 -0700 (PDT)

(*The Vancouver Sun*, 27 Jun 2002)

Four anglers were rescued by helicopter Wednesday from a small island in the Capilano River after a control malfunction at the Greater Vancouver regional district's Cleveland Dam released an unexpected torrent of water. The malfunction of the drum-gate water-control mechanism, which occurred during a computer upgrade, is expected to prompt the installation of more signs along the river warning fishermen of the potential for rapid increases in water levels.

The Cleveland Dam had been releasing snow-melt water through the drum-gate at the rate of about 1,000 cubic feet per second when the malfunction occurred at 7 a.m. Wednesday. By the time dam employees brought the problem under control about an hour later, the flow had increased four-fold to about 4,000 cubic feet per second. At that rate, it would take about 30 seconds to fill an Olympic-sized swimming pool.

Thomas Dzubin note: the GVRD does not tightly control physical access to the land around the Capilano river and I've walked by various points along its banks quite a few times. I guess the Risk here might be that you shouldn't automate a system where you can't control access to all directly affected points or at least have an independent feedback system in place to not allow (or send an alarm) a 4x increase in flow over a short period of time. (Although, I'm not a civil engineer...such a feedback mechanism might be tough to implement and still allow the dam to "let-go" water in emergency situations such as the week-long rainstorms which we

sometimes have in Vancouver.)

Thomas Dzubin, Vancouver, Calgary, or Saskatoon, CANADA

China bans toxic American computer junk

Mich Kabay <mkabay@compuserve.com>

Sun, 30 Jun 2002 11:24:34 -0400

John Gittings in Shanghai, writing for the Guardian Weekly, published an article entitled "China bans toxic American computer junk: Electronic scrap puts the lives of rural villagers at risk" (GW, 2002-06-01, <<http://www.guardian.co.uk/international/story/0,3604,725756,00.html>>).

"Beijing has announced a clampdown on the import of electronic junk from the US and other developed countries which is being stripped by Chinese peasants in primitive and dangerous conditions.

The ban follows an outcry by western environmental groups and in the Chinese press about reports that young children are employed to smash up computers and that local water supplies have been poisoned by toxic waste.

A new list of banned items will include "TV sets, computers, Xerox machines, video cameras and telephones", according to the national environment agency."

The article goes on to describe threats to the health of >100,000 unprotected workers, including children, who extract heavy

metals from
circuit boards plus severe environmental degradation to farmland
surrounding
the recycling centers. Most of the waste comes from the US
because, "The US
is the only industrialised country to have failed to ratify the
1989 UN
Basel convention which calls for a total ban on the export of
hazardous
waste."

This article highlights the RISKS of assuming that bringing our
defunct computer gear to a recycling center is "protecting the
environment." It may be protecting our part of the environment,
but
on a global basis, we seem to be causing a great deal of harm to
many
poor people and to the long-term future of our planet. In
addition,
we ought to look at the morality of treating other human beings
as if
they are expendable tools for protecting ourselves at their
expense.

Seems to me that the only sustainable approach to reducing the
harm we can
cause by discarding computer gear is to include the price of
safe recycling
in the purchase price and to have manufacturers, wholesalers and
retailers
contribute to an economically viable treatment process where
users live --
not in some shantytown on the far side of the planet. Perhaps
signing and
abiding by the Basel convention would be a good first step.

M. E. Kabay, PhD, CISSP, Dept CompInfoSys, Norwich University,
Northfield VT

<http://www2.norwich.edu/mkabay/index.htm>

A Microsoft Medley in [RISKS-22.13](#)

Peter da Silva <peter@abnm.com>

Thu, 4 Jul 2002 18:22:20 -0500 (CDT)

Four fascinating articles in [RISKS-22.13](#):

> Microsoft's secret plan to secure the PC (Monty Solomon)

The referenced article included such gems as "Palladium stops viruses and worms. The system won't run unauthorized programs, preventing viruses from trashing your system." Setting aside all the other issues in the article, this by itself is a remarkable piece of misdirection.

Why? Well, let's look at viruses...

There are four main avenues that viruses and worms use to spread. There are others, but the vast majority of outbreaks have used these avenues of attack.

The first, and oldest, is "social engineering". You trick a human into running a program for you. This is the electronic equivalent of calling up the sysop at a company and saying "hey, this is Jack Smith in accounting, I can't get in, I forgot my password because I had it programmed into my mail program, can you clear it for me?". Making the OS more secure can help somewhat, but you don't need to wait for Palladium to do this... most multi-user operating systems are designed so that users normally run with restricted privileges, and so can only damage their own files... not the OS or other user's programs.

The second is exploiting a straightforward bug, usually a buffer

overflow. To fix this you don't need a new security model, you need a programming language that doesn't allow buffer overflows.

The third is a "cross frame attack": you trick the client software (web browser, e-mail program, music player) into running untrusted code without restrictions. This is almost always an attack on Microsoft's poorly-advised merge of the web browser (which is almost always dealing with untrusted objects) with the desktop, mail software, and so on. If they had integrated the HTML rendering engine in the OS and left the Internet access code in a separate program that used the HTML rendering code but otherwise managed its own access controls... at least 90% of the widespread virus outbreaks would never have happened.

The fourth is conversion attacks. You encode the message containing the attack code inside a package the outer layers of the OS or application don't know how to open. Ironically, Palladium is likely to make this kind of attack easier, because it's almost certain that part of the security model will involve separating the system up into components that don't have the keys to each other's files.

Ironically, one of the latest security issues with a Microsoft product is due to the first Palladium-type software having three of the kind of security holes I just listed above... Windows Media Player. The second of the three holes would not exist if Media Player didn't have to have access to the OS internals to implement Digital Rights

Management.

Of more concern, the integration of the browser and the desktop and other components that created the possibility of "cross frame attacks" is due specifically to Microsoft's attempt to avoid complying with their original agreement with the Justice Department by bundling the Browser and the OS. Microsoft has maintained this dangerous design despite years of massive virus outbreaks caused by this decision, because otherwise they'd have to admit fault. Even now, when they have been found at fault, and there's nothing left to lose, they refuse to unbundle the Internet access from the rendering code.

So, not only has Microsoft never before shown much concern for this problem, they have actively worked to prevent a straightforward fix that they are legally required to implement. Using this issue as a hook to get more control of the computer is, well, there are polite terms for it and I'll let you decide which one to apply.

Even if you don't care about this specific issue, what does this say about their likely behaviour if security problems crop up in the design of Palladium?

- > Risks to your privacy from using MSN Messenger 4.6? (Michael Weiner)
- > Microsoft sent Nimda worm to developers (Mike Hogsett)

The implications of these two, in light of the first, are obvious.

- > Microsoft's Allchin: API disclosure may endanger U.S. (Brien

Webb)

This article basically says that Microsoft knows they have fundamental design flaws in their protocols, which if discovered will open up your computer to uncontrolled access.

So now they want us to trust them that this time, honest, they'll really get it right?

⚡ Windows Media Player security update EULA gives MS permission to keep

Bill Tolle <BillTolle@ExclusiveBuyersAgents.com>

Sun, 30 Jun 2002 10:56:11 -0500

you from using "other software" on your computer

The latest from MS is buried deep in the EULA if you download the Windows Media Player security update:

"You agree that in order to protect the integrity of content and software protected by digital rights management ('Secure Content'), Microsoft may provide security related updates to the OS Components that will be automatically downloaded onto your computer. These security related updates may disable your ability to copy and/or play Secure Content and use other software on your computer. If we provide such a security update, we will use reasonable efforts to post notices on a web site explaining the update."

"may disable your ability to copy and/or play Secure Content and use other software on your computer" is an interesting phrase. If you remove one item from the sentence it becomes "may disable your ability to use other software on your computer".

Wonder what "other software" Bill G. might decide to not let us use at some point in the future?

See <http://www.theregus.com/content/4/25435.html>

Bill Tolle <BillTolle@ExclusiveBuyersAgents.com>

⚡ Re: E-mail address parsing {[RISKS-22.13](#)}

George Roussos <gr@dcs.bbk.ac.uk>
Mon, 1 Jul 2002 00:28:08 +0100 (BST)

>The risk is that the customer-relations programmers are living in a world of [a-z0-9_] for mailbox names, while the standard has long allowed for virtually any character (including NULL).

Actually, they live in an MS Outlook world (try to send e-mail to "@ @"@nmt.edu using outlook). In fact, Outlook would refuse to send e-mail to a number of perfectly valid addresses, including any that contain the end dot for the root domain. This is obviously a feature, not a bug!

⚡ MI5 hates encryption so much, they don't use it!

Ben Laurie <ben@algroup.co.uk>

Wed, 03 Jul 2002 12:39:06 +0100

According to Network News (the UK rag) today, MI5, the Home Office, and others don't use PGP signing at RIPE (the European Internet registry), although its the only really secure method for updating records. So anyway, I thought I'd look into it, and, well, its true (edited highlights follow):

```
www.mi5.gov.uk.          6715      IN        A         128.98.11.23
```

```
inetnum:                128.98.0.0 - 128.98.255.255
```

```
mnt-by:                 QINETIQ-UK-MNT
```

```
mntner:                 QINETIQ-UK-MNT
```

```
auth:                   MD5-PW $1$tSMW1DGk$GIAERGLu5BwBUXabmYjvs1
```

I'm sure Qinetiq haven't been so foolish as to choose a guessable password (after all, they've shown their IT expertise by the masterly handling of the 1901 Census website), but even so, their e-mail must contain the password in plain text. Of course, if anyone out there runs their password cracker on that and finds I'm wrong, I'd love to hear about it.

Note: all data above is from publicly available sources.

Incidentally, the article suggests that some people are still using MAIL-FROM auth, which is, frankly, astonishing. I can't be bothered to track down who, though.

Ben <http://www.apache-ssl.org/ben.html> <http://www.thebunker.net/>

```
[PS. OK, I lied: I can be bothered. This is just too amazing:
www.gov.uk.          35656   IN      CNAME   www.ukonline.
gov.uk.
www.ukonline.gov.uk.  283     IN      A       195.33.102.13

inetnum:             195.33.96.0 - 195.33.127.255
mnt-by:              AS12967-MNT

mntner:              AS12967-MNT
auth:                MAIL-FROM .*@att.nl
auth:                MAIL-FROM .*@icoe.att.com
```

Yes, folks. The UK government's Website uses MAIL-FROM auth.
And not even
.uk addresses!]

🔥 More on The Telecom Crash of 2002

Dave Farber <dave@farber.net>
Sun, 30 Jun 2002 19:15:06 -0400

```
----- Forwarded Message
>Date: Sun, 30 Jun 2002 12:00:36 -0700
>From: "Joseph C. Pistritto" <jcp@jcphome.com>
>Subject: Re: IP: The Telecom Crash of 2002
```

The most telling comment here is the comment about bankruptcy allowing new players to take over bandwidth debt-free, dropping prices.

We've seen this pattern before. In Iridium for instance. Further, we see it in the equipment markets, where companies can buy equipment on the secondary market for 20% of list price. This is hurting all the equipment companies as well. (especially Sun, which is very vulnerable to this.) Cisco is probably hurting as well because of it.

Its an interesting vicious circle:

- 1) People install something, (bandwidth, satellites, Sun machines, etc.) and don't have enough revenue to support the cost of it.
- 2) They go into debt, sometimes spectacularly
- 3) They go bankrupt servicing the debt, which gets written off.
- 4) Other people buy the assets debt-free, and can now cut prices
- 5) Driving all other providers to go into *more* debt. (if they can), or go bankrupt (if they can't).
- 6) Making more of them go bankrupt. - iterate to step (3).

This can't stop until everyone's gone through bankruptcy, to get back on a "level" playing field.

As a programmer at heart, I have to believe there's a bug here.

Its clear that the worst iterations of this are where the item involved can only be used to provide *one kind* of service. If it's Sun machines, companies could buy them to put in their internal networks, they don't have to only build e-~~something~~ web sites with them. But with Telecom bandwidth, you're stuck. Fiber only moves bits. Voice bits or Data bits, but still bits. Which is why this bug is much worse for the Telecom people than for other kinds of equipment makers, which have multiple non-competitive uses. jcp

Dave's archives:

<http://www.interesting-people.org/archives/interesting-people/>

✶ Security in General - wireless - simplicity

msimon <msimon@xta.com>

Thu, 27 Jun 2002 12:33:50 +0100

I think that wireless networks and www based networks for hardware control are a thing of the past.

I had often thought that this was the stupidest thing I had ever heard of and so despite the personal cost had never bothered to learn the technology.

Sadly events are beginning to prove me correct. I expect my retro skills to be in high demand shortly.

Remember the days when everything was going to be hooked up to the net? Let us hope those days are gone for good.

Wires and hard connections. Still vulnerable but at least you need physical access.

No doubt this will raise costs. But you have to balance that against what a plant is worth. I am aware of new aircraft designs that are using IP for moving data in an aircraft rather than a proprietary protocol as was usual in the past. Dumb, dumb, dumb.

BTW I worked on the original Raytheon ATC when I got out of the Navy in '67. It is interesting to see how badly Raytheon has bungled the replacement. If only they had gone with advanced hardware capable of future expansion and simply directly replaced the old terminals and systems 1:1. No bells and whistles. Then once they had the simple

replacements proved start doing revs. But no - like all fools they got too ambitious. All they could see was how much money and how much more capable the new system was going to be. And in C yet. Where you are at the mercy of the compiler writer rather than the now relatively defunct FORTH system which produces code that is always defined the same way in every instance and is much easier to test.

Simpler is better. But try telling that to any young fool who never fought in the clone wars.

FORTH

msimon <msimon@xta.com>

Thu, 27 Jun 2002 13:00:23 +0100

Did I mention that FORTH could be the assembly language of a relatively simple processor?

The advantage is that you get a language on a par with C that runs directly on the processor.

I know of no processor that runs C code directly. You need a relatively complex compiler and lots of hardware tricks to make it run fast.

The compiler becomes untestable because of all of the possible combinations and the million transistor chips become untestable for the same reason.

The FORTH model is a simple processor (30,000 transistors for 16

bit -

100,00 transistors for 32 bit) with lots of stack and local memory.

Memory is very testable. So are simple processors. Because of the simplicity of design the FORTH chip needs only a one level deep pipeline

and no branch predictors since a pipeline miss only costs you one cycle

at most. Sometimes depending on the code there is no penalty. A few

years back they were getting speeds of 500 MIPS from 1 micron design

rules and a 32 bit wide bus. Instructions were 5 bits so you got 6

instructions per fetch (best case). With a memory rate of 90 million

fetches a second. Go to 64 bits if you need to reduce the external

memory rate to a very comfortable 45 million fetches a second.

But every one today is in love with complexity. Stupid, stupid, stupid.

Except from a marketing standpoint. Yechh.

Did I mention that all the new complexity requires a very expensive and hard

to test and verify BGA package for all the interconnects vs a less dense

PQFP type package that is visually inspectable vs X-ray inspection which

degrades the silicon.? Yechh again.

But no one listens to me. I'm not bleeding edge enough. Too simple.

11th USENIX Security Symposium

Alex Walker <alex@usenix.org>

Mon, 01 Jul 2002 15:08:08 -0700

San Francisco. Check out <http://www.usenix.org/sec02> for our early registration and student discounts.

This year's program brings together an exceptional group of speakers to inform and educate including Keynote speaker Whitfield Diffie, co-inventor of public key cryptography and Chief Security Officer at Sun Microsystems. Diffie will talk about security policy and challenges for the 21st century. Other Invited Talks teach you why common security systems fail; how to validate and test security designs; how to make biometrics authentication work; legal aspects of the DMCA; and much more.

For detailed information and to register, please visit our Web site at: <http://www.usenix.org/sec02>

Alex Walker, Production Editor, USENIX Association
2560 Ninth Street, Suite 215, Berkeley, CA 94710
1-510-528-8649 x33

🔥 REVIEW: "Decrypted Secrets", F. L. Bauer

Rob Slade <rslade@sprint.ca>
Tue, 25 Jun 2002 07:44:48 -0800

"Decrypted Secrets", F. L. Bauer, 2002, 3-540-42674-4, U\$44.95
%A F. L. Bauer
%C 175 Fifth Ave., New York, NY 10010
%D 2002
%G 3-540-42674-4
%I Springer-Verlag
%O U\$44.95 212-460-1500 800-777-4643 rjohnson@springer-ny.com

%P 474 p.

%T "Decrypted Secrets: Methods and Maxims of Cryptology, 3rd Ed."

Cryptology is the study of the technologies of taking plain, readable text, turning it into an incomprehensible mishmash, and then recovering the initial information. There are two sides to this study. Cryptography is the part that lets you garble something, and then recover it if you have the key. Cryptanalysis is usually seen as the "dark side" of the operation, because it is the attempt to get at the original meaning when you *don't* have the key. Most current and popular works on cryptology actually only speak about cryptography. For one thing, nobody wants to get into trouble by telling people how to break encryption. However, it is also much easier to blithely talk about key lengths and algorithms and pretend to know what you are doing than it is to demonstrate a sufficient mastery of mathematics to enable you to go about cracking a particular cipher.

Bauer examines both sides, which is an important plus. If you need to decide how strong an encryption algorithm or system is, it is important to know how difficult it might be to break it.

Chapter one looks at steganography, the science of hiding in plain sight, or concealing the fact that a message exists at all. In this he first demonstrates a wide ranging historical background which is quite fascinating in its own right. Basic encryption concepts are introduced by the same historical background, but move on to a very dense mathematical discussion of cryptographic characteristics in

chapter two. Encryption functions are started in chapter three, and it is delightful to have examples other than Julius Caesar's substitution code. Polygraphic substitutions are in chapter four and the math for advanced substitutions is in chapter five. Chapter six introduces transpositions. Families of alphabets, and rotor encryptors such as ENIGMA, are reviewed in chapter seven. Keys are discussed in chapter eight, ending with a brief look at key management. Chapter nine covers the combination of methods resulting in systems such as DES (Data Encryption Standard). The basics of public key encryption are introduced in chapter ten. The relative security of encryption is introduced in chapter eleven, leading to part two. However, Chapter eleven also ends with a discussion of cryptology and human rights, concentrating mainly, although not exclusively, on the US public policy debates.

Part two examines the limits of functions used in cryptography, and thus the points of attack on encryption systems. Chapter twelve calculates complexity, and thus the size of brute force attacks. Known plaintext attacks are the basis of chapters thirteen to fifteen, looking first at general patterns, then at probable words, and finally at frequencies. Frequency leads to a discussion of invariance in chapter sixteen. Chapter seventeen follows with a look at key periodicity. Alignment of alphabets is covered in chapter eighteen. Of course, cryptographic users sometimes make mistakes, and chapter nineteen reviews the different errors and various ways to take advantage of them. Chapter twenty one looks at anagrams as an effective attack on transposition ciphers. The concluding chapter muses on the relative effectiveness of attacks and of cryptanalysis overall.

Those seriously interested in cryptology will really *need* to be serious: brush up on your number theory if you want to use this book

for anything. This third edition is essentially and structurally unchanged from its predecessors, although it has been updated to reflect the latest algorithms and technologies. Bauer's history and vignettes from the story of codes and the codebreakers are interesting, amusing, and accessible to anyone.

copyright Robert M. Slade, 1998, 2002 BKDECSEC.RVW 20020520
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

<http://victoria.tc.ca/techrev> or <http://sun.soci.niu.edu/~rslade>



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

[ACM](#) Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 15

Sunday 14 July 2002

Contents

- [Listen to TCAS, not the controller!](#)
[Monty Solomon](#)
- [Biometric programs "more ... toys than of serious security measures"](#)
[Yves Bellefeuille](#)
- [Brazilian Internet theft](#)
[Tom Van Vleck](#)
- [Pretty Poor Privacy from Network Associates](#)
[NewsScan](#)
- [FreeBSD Scalper worm, a bad precedent...](#)
[Nicholas C. Weaver](#)
- [Software bugs cost the US 40bn a year](#)
[Pete Mellor](#)
- [Free Prozac in the junk mail draws a lawsuit](#)
[Monty Solomon](#)
- [Cringely on Palladium](#)
[Pete Mellor](#)
- [More on Palladium](#)
[Pete Mellor](#)
- [EULA](#)
[Monty Solomon](#)

- [Windows Media Player security update EULA](#)
[Pedt Scragg](#)
 - [Re: Randomly generated 4-letter words in sendmail ...](#)
[Bill Gunshannon](#)
 - [Re: US Navy suffers domain hijacking](#)
[Bill Stewart](#)
[Conor O'Neill](#)
 - [Re: E-mail address parsing](#)
[Tony Finch](#)
 - [Re: FORTH](#)
[Jonathan](#)
 - [REVIEW: "Digital Signatures", Mohan Atreya et al.](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Listen to TCAS, not the controller!

Monty Solomon <monty@roscom.com>

Wed, 10 Jul 2002 01:31:45 -0400

Edmund L. Andrews: Controller Sent Jets Into Crash, Flight Data Show

**The New York Times*, 9 July 2002*

Information from the flight recorders aboard the two planes that crashed into each other one week ago over southern Germany show that a Swiss air traffic controller in effect put the planes on a collision course by ordering the Russian pilot to descend at the same time that the plane's own collision-avoidance system was urging him to climb.

The new data, released today by German investigators, show that the two planes' automated systems communicated with each other exactly

as they were meant to do and that the accident would probably not have occurred if the Russian pilot had simply ignored the Swiss controller in Zurich. The collision killed 52 Russian schoolchildren and 19 adults.

In addition, German investigators said German controllers saw danger nearly two minutes before the crash and desperately tried to warn the controllers in Zurich, who had responsibility for both planes. ...

<http://www.nytimes.com/2002/07/09/international/europe/09CRAS.html>

⚡ Biometric programs "more ... toys than of serious security measures"

Yves Bellefeuille <yan@storm.ca>
Sat, 06 Jul 2002 03:05:13 -0400

Since the death of `_Byte_`, the German magazine `_c't_`, or `_Magazin fuer Computer Technik_`, is probably the best technical computer magazine in the world.

Some articles from this magazine are translated into English and made available on its WWW site at <http://www.heise.de/> . One recent article of interest to comp.risks readers is "Biometric Access Protection Devices and their Programs Put to the Test", from `_c't_` 11/2002, dated 22 May 2002, available at <http://www.heise.de/ct/english/02/11/114/> .

The conclusion is that "the products in the versions made available to us were more of the nature of toys than of serious security measures".

One wonders whether the biometric security programs now used by corporations and governments, especially in the US, are any better.

Yves Bellefeuille <yan@storm.ca>, Ottawa, Canada

Esperanto FAQ: <http://www.esperanto.net/veb/faq.html>

Rec.travel.europe FAQ: <http://www.fags.org/fags/travel/europe/faq>

🔥 Brazilian Internet theft

Tom Van Vleck <thvv@multicians.org>

Fri, 12 Jul 2002 14:24:38 -0400

Arrest of hacker is requested

Jornal do Brasil, Sexta-Feira, 12 Jul 2002

(tvv rough translation, thanks babelfish)

The police of Mato Grosso do Sul yesterday asked for the re-arrest of the student Guillermo Amorim de Oliveira Alves, age 18 years, accused of the biggest theft yet carried out through the Internet in Brazil. Guillermo was arrested 19 Jun 2002 in the act of diverting R\$25,000 from bank accounts using a notebook computer. He was held in custody for 14 days by the Federal Police and was released on 3 Jul on habeas corpus. But analysis of his computer, divulged on 9 Jul, showed that the hacker violated the sites of four national banks and diverted at least R\$120,000 from 50 accounts.

The analysis is incomplete, but there is evidence that the hacker has a bank account containing R\$3 million. His computer also contained 3500 American credit-card numbers from two card issuers. The FBI will enter the case.

✶ Pretty Poor Privacy from Network Associates

"NewsScan" <newsscan@newsscan.com>

Fri, 12 Jul 2002 09:44:27 -0700

A computer security company has uncovered a flaw in PGP (Pretty Good Privacy) -- a freely distributed, public key encryption system that's used to scramble e-mail messages -- that could allow malicious users to unscramble sensitive messages. The flaw is found only in PGP plug-ins for Microsoft Outlook users distributed by Network Associates. "The PGP vulnerability enables an attacker to send a specially crafted e-mail to any Outlook address enabled with the PGP plug-in, which will in turn give them access to that system," says eEye Digital Security, which discovered the problem. EEye chief hacking officer Marc Maiffret says the flaw allows an attacker to do "anything a user of that machine could do -- copy files, delete files, install a backdoor." Gartner research director for Internet security John Pescatore says, "This vulnerability means people using [the affected] version of PGP actually are less secure than if they weren't using security at all. It's always a really, really bad thing when a

security

product has a bug." (NewsFactor Network, 11 Jul 2002; NewsScan Daily, 12 Jul 2002)

<http://www.ecommercetimes.com/perl/story/18560.html>

✶ FreeBSD Scalper worm, a bad precedent...

"Nicholas C. Weaver" <nweaver@CS.Berkeley.EDU>

Mon, 8 Jul 2002 15:31:11 -0700 (PDT)

The recent Apache "scalper" worm, targeting FreeBSD systems, represents a dangerous precedent, even if it is a rather ineffective worm: it linearly scans randomly selected class Bs, it doesn't employ a very good scanner, and it can only infect a few types of machines (Apache 1.3.20, .22-24 running on FreeBSD).

It was roughly 10 days between when Gobbles Security released an exploit for the recent Apache vulnerability (in response to ISS's statement two days earlier, announcing the vulnerability and stating that it was only exploitable on win32 and some 64 bit platforms) that the worm was seen in the wild. This compared with several months for Code Red and Nimda, between vulnerability disclosure and appearance of a worm.

We can expect this time to reduce to nearly 0 in the future, as worm authors prepare worms in advance, or borrow existing worm code, and simply drop in exploits as they are published. As we have already seen mail

worm toolkits,
we can expect similar active scanning worm toolkits. This means
that the
window of vulnerability between when an exploit or flaw is
published, and
when it is actively exploited, will quickly reduce to zero.

As important, this worm contained a controllable DOS and
backdoor module,
something directly useful to a blackhat, as did the Goner mail
worm. The
blackhat community has realized that worms are a great way to
compromise
machines with little effort and little risk.

My personal, somewhat hazy crystal ball: Over the next year, we
will see a
lot of "1 day" worms, where shortly after an exploit is
published, a
corresponding worm will be released. These worms will almost
invariably
carry DDoS, credit card searchers, or similar payloads optimized
for
blackhat goals. We probably will see toolkits!

We will also start to see worms appearing less than 2-3 days
after a
detailed vulnerability is reported, as slightly more
sophisticated blackhats
create an exploit, drop it into existing frameworks, and release
worms.

Be Afraid (tm).

Scalper Worm code and first detection was at
<http://www.dammit.lt/apache-worm/>

Nicholas C. Weaver <nweaver@cs.berkeley.edu>

Software bugs cost the US 40bn a year

Pete Mellor <pm@csr.city.ac.uk>

Sat, 29 Jun 2002 14:30:27 +0100 (BST)

I tried to look for a reference to the original NIST report, but could not access www.nist.gov at the time.

Computer Weekly, 28 June 2002

<http://www.cw360.com/article%26rd%3D%26i%3D%26ard%3D113682%26fv%3D1>

Software bugs are costing the US economy an estimated 40bn [pounds?] each year, with almost two-thirds of the cost being borne by end-users, and the remainder by developers and vendors, according to a new study for the US government. Software faults could be costing the European Union, whose 15 member states have a combined gross domestic product (GDP) slightly less than the US GDP almost as much again. The US study, by the National Institute of Standards and Technology (NIST), said that testing could reduce the cost of bugs by about a third but would not eliminate all software errors.

Free Prozac in the junk mail draws a lawsuit

Monty Solomon <monty@roscom.com>

Sun, 7 Jul 2002 11:56:44 -0400

Unsolicited Prozac arrived in a hand-addressed manila envelope, from a nearby Walgreens drugstore, with a "Dear Patient" form letter.

"Enclosed

you will find a free one month trial of Prozac Weekly.

Congratulations on

being one step to full recovery." This led one recipient to file a

class-action lawsuit, stating that Walgreens, a local hospital, three

doctors, and Prozac's maker Eli Lilly misused patients' medical records and

invaded their privacy. It also accused the drugstore and Lilly of engaging

in the unauthorized practice of medicine. [PGN-ed from article by Adam

Liptak, *The New York Times*, 6 Jul 2002]

<http://www.nytimes.com/2002/07/06/national/06PROZ.html>

Cringely on Palladium

Pete Mellor <pm@csr.city.ac.uk>

Tue, 9 Jul 2002 22:49:37 +0100 (BST)

Those who have been following the Palladium thread might be interested in

the following article entitled "I told you so" by Robert X. Cringely:-

<http://www.pbs.org/cringely/pulpit/pulpit20020627.html>

The following is a long extract from his article:

Let's concentrate on the Microsoft story. Last August, I wrote of a rumor

that Microsoft wanted to replace TCP/IP with a proprietary protocol -- a

protocol owned by Microsoft -- that it would tout as being more secure.

Actually, the new protocol would likely be TCP/IP with some of the

reserved fields used as pointers to proprietary extensions, quite similar

to Vines IP, if you remember that product from Banyan Systems. I called it TCP/MS in the column. How do you push for the acceptance of such a protocol? First, make the old one unworkable by placing millions of exploitable TCP/IP stacks out on the Net, ready-to-use by any teenage sociopath. When the Net slows or crashes, the blame would not be assigned to Microsoft. Then ship the new protocol with every new copy of Windows, and install it with every Windows Update over the Internet. Zero to 100 million copies could happen in less than a year.

This week, Microsoft announced Palladium through an exclusive story in Newsweek written by Steven Levy, who ought to have known better. Palladium is the code name for a Microsoft project to make all Internet communication safer by essentially pasting a digital certificate on every application, message, byte, and machine on the Net, then encrypting the data EVEN INSIDE YOUR COMPUTER PROCESSOR. Palladium compatible hardware (presumably chipsets and motherboards) will come from both AMD and Intel, and the software will, of course, come from Microsoft. That software is what I had dubbed TCP/MS.

The point of all this is simple. It may actually make the Internet somewhat safer. But the real purpose of this stuff, I fear, is to take technology owned by nobody (TCP/IP) and replace it with technology owned by Redmond. That's taking the Internet and turning it into MSN. Oh, and we'll all have to buy new computers.

This is diabolical. If Microsoft is successful, Palladium will give Bill

Gates a piece of every transaction of any type while at the same time

marginalizing the work of any competitor who doesn't choose to be

Palladium-compliant. So much for Linux and Open Source, but it goes even

further than that. So much for Apple and the Macintosh. It's a militarized

network architecture only Dick Cheney could love.

Ironically, Microsoft says they will reveal Palladium's source code, which

is little more than a head feint toward the Open Source movement. Nobody

at Microsoft is saying anything about giving the ownership of that source

code away or of allowing just anyone to change it.

Under Palladium as I understand it, the Internet goes from being ours to

being theirs. The very data on your hard drive ceases to be yours because

it could self-destruct at any time. We'll end up paying rent to use our

own data!

Can you tell I think this is a bad idea?

What bothers me the most about it is not just that we are being sold a

bill of goods by the very outfit responsible for making possible most

current Internet security problems. "The world is a fearful place (because

we allowed it to be by introducing vulnerable designs followed by clueless

security initiatives) so let us fix it for you." Yeah, right. Yet

Palladium has a very real chance of succeeding.

How long until only code signed by Microsoft will be allowed

to run on the
platform? It seems that Microsoft is trying to implement a
system that
will enable them, once and for all, to charge game console-
like royalties
to software developers.

✶ More on Palladium

Pete Mellor <pm@csr.city.ac.uk>

Fri, 12 Jul 2002 12:59:22 +0100 (BST)

My thanks to the person who sent me the forwarded message
below. (I have
withheld his name just in case, although the URL he sent is a
totally public
source.)

Please have a look at both of the URLs below.

My informant is right: if the Cringely article scared you, after
reading
Ross Anderson's contribution, you'll turn green and have to
change your
pants!

PS: It is not made clear in the article, but Ross Anderson is a
very highly respected computer security guru at Cambridge
University.

----- Forwarded message -----

Date: Thu, 11 Jul 2002 19:06:12 +0100

Subject: more palladium stuff

Dear Colleagues,

As a follow-up of Pete Mellor's mail "Cringely on Palladium ",
here's
another document, which is WAY more scary than what he sent:

<http://www.cl.cam.ac.uk/users/rja14/tcpa-faq.html>

I think everybody who is involved in computer stuff should read it...

especially programmers and software developers!!! This information should

be spread widely and people should know about it!!! Forward this to your friends!

For those of you, who haven't received Pete Mellor's mail, here's the link to the document he sent (you may want to READ IT FIRST):

<http://www.pbs.org/cringely/pulpit/pulpit20020627.html>

EULA

Monty Solomon <monty@roscom.com>

Thu, 11 Jul 2002 23:35:55 -0400

Excerpt from

<http://www.macintouch.com/toasttitanium3.html>

>Date: Wed, 10 Jul 2002s

>From: [MacInTouch Reader]

>Subject: Roxio Toast 5.1.4. Update EULA language

>Like many people who use a computer daily, I prefer to keep my software

>up to date. And so I generally utilize updates provided by the various

>software manufacturers.

>However, given recent reports of Microsoft's impending Palladium

>technology and its ability to invade a computer at will, I've taken to

>actually reading the license agreements that one must accept in order to
>install software or updates.

>Just a few days ago, I retrieved the v5.1.4 update for Roxio's Toast CD
>mastering software. And was stunned to discovered the following verbiage
>emplaced within the license agreement's "RESTRICTIONS" section.

>Content providers are using the digital rights management technology ("DRM")
>contained in this Software to protect the integrity of their content
>("Secure Content") so that their intellectual property, including copyright,
>in such content is not misappropriated. Owners of such Secure Content
>("Secure Content Owners") may, from time to time, request Roxio or its
>suppliers to provide security related updates to the DRM components of the
>Software ("Security Updates") that may affect your ability to copy, display
>and/or play Secure Content through the Software or other applications that
>utilize the Software. You therefore agree that, if you elect to download a
>license from the Internet which enables your use of Secure Content, Roxio or
>its suppliers may, in conjunction with such license, also download onto your
>computer such Security Updates that a Secure Content Owner has requested
>that Roxio or its suppliers distribute. Roxio and its suppliers will not
>retrieve any personally identifiable information, or any other information,
>from your computer by downloading such Security Updates.

>Note that these statements are nestled in the midst of a longer paragraph
>containing the usual stuff about not reverse engineering the

software, with
>copy not directly related to these statements preceding and
following these
>statements. Almost as if Roxio hoped that this language would
not be
>noticed.

>I'd suspected something like this might be present within the
agreement ever
>since a recent session of burning music CD's from my collection
of MP3's,
>using Toast v5.1.3. The last discs I burned play normally, both
on my
>computer and in my CD players, but if you put one of them into
the
>computer's drive and open it as a data disc, you are presented
with a list
>of untitled files, all zero mb in length.

>I haven't tried to copy one these discs, as I've no reason to
do so as yet.
>And as I still have my mp3 files, I can make another whenever
needed.

>But with this discovery, I find myself hoping for a viable
alternative to
>Toast.

>Note here that I use an older Mac, a Performa 6360, upgraded
with a Sonnet
>G3/320 L2 card. Apple's DiscBurner software will not load,
stating that it
>requires a machine with built-in USB capability. I have not
been able to
>utilize iTunes' burning capability, either, which requires OS
9.2 and 9.2
>updates refuse to install on my machine.

Windows Media Player security update EULA (Re: Tolle, [RISKS-](#)

22.14)

Pedt Scragg <bofh@pkuatb.net>

Sun, 14 Jul 2002 07:27:32 +0100

> "may disable your ability to copy and/or play Secure Content
> and use other
> software on your computer" is an interesting phrase. If you
> remove one
> item from the sentence it becomes "may disable your ability to
> use other software on your computer".

AV software in case MS accidentally send out another virus,
firewalls to
allow MSN Messenger et al. free reign?

There is a further risk here in the item that Bill removed from
that
sentence. For example, updated software looking at software
version numbers
refusing to allow plain text e-mailed content to be 'copied' to
the updated
recipient machine if the source is software which has not been
updated to a
version which included this new bit of the EULA.

A second risk became evident when this new bit of the EULA was
discussed
in a newsgroup when all the posters after the original article
stated
they didn't apply any security patches.

✶ Re: Randomly generated 4-letter words in sendmail ... (Ake, [R-22.13](#))

Bill Gunshannon <bill@cs.scranton.edu>

Mon, 8 Jul 2002 08:19:31 -0400 (EDT)

A more interesting concern is the encoding used by MIME. Things like UUencode and BASE64 (and others, I am sure) create extremely large files of random (at least as far as language is concerned) letters. When I search some of my saved mail folders I can find pretty much any 3 or 4 letter combination. I have even mentioned in discussions around the department the concept that as the number of viruses increases and the amount of encoded e-mail increases the number of false positives will also have to increase. When you add "dirty word" filtering to the equation matters become much worse. In a system that automatically discards suspect e-mail, this could mean a lot of important information not getting through.

Bill Gunshannon, University of Scranton, Scranton, Pennsylvania
<bill@cs.scranton.edu>

✉ **Re: US Navy suffers domain hijacking (Brent, [RISKS-22.10](#))**

Bill Stewart <bill.stewart@pobox.com>

Sat, 06 Jul 2002 17:01:57 -0700

The United States Post Office is well-known for its confusion about whether it wants to be treated as a business or a government agency.

The Louisiana Attorney General's office, however, by using the domain la-ag.com a couple years ago, was clearly stating that it's in business.

Not sure what business it's in, or what its prices are :-)

The domain is now owned by some agricultural company, which makes more sense, and the LA AG's office is using www.ag.state.la.us/

⚡ Re: US Navy suffers domain hijacking (Ashworth, [RISKS-22.13](#))

"Conor O'Neill" <ONeillCJ@logica.com>

Tue, 9 Jul 2002 09:30:50 +0100

Similarly, the UK parliament has a perfectly good Web address:

<http://www.parliament.uk/>

but insists on using a .tv suffix for its live video feed:

<http://www.parliamentlive.tv/>

Conor O'Neill, Bristol, UK

⚡ Re: E-mail address parsing (Colburn, [RISKS-22.13](#))

Tony Finch <dot@dotat.at>

Fri, 12 Jul 2002 17:41:09 +0100

[I have excerpted starkly from an extended exchange between George Roussos and Tony Finch, inspired by Colburn. PGN]

You should read this in the context of the syntax for domains in RFC

821 and 822 (or rather 2821 and 2822 if you want to be up-to-date),

which does not allow a . at the end of the domain.

> In practice, I have not come across a mailer that would not recognise

> or refuse delivery when the root dot is present, including all
versions
> of exchange (please check this, it is true).

Sendmail and Exim are popular MTAs [that consider the dot
invalid].

[Examples omitted. PGN]

Other MTAs might not care if you violate the RFCs.

f.a.n.finch <dot@dotat.at> <http://dotat.at/>

✉ Re: FORTH (Simon, [RISKS-22.14](#))

Victor the Cleaner <jonathan@canuck.com>

Tue, 9 Jul 2002 14:31:27 -0600

Sadly, as a more recent trend that's true. For a while, some
folks were on
this track, though. Back in the early 80s, Rockwell had a
couple of parts
(65F11 and 65F12, IIRC) that had a Forth interpreter in mask
ROM; New Micros
(newmicros.com) still sells a 68HC11 with onboard Forth. And in
the
late-80s Harris sold a part (licensed from Novix, I think) that
was a really
speedy little thing optimized for Forth (with heavy emphasis on
the stack).

More information at: <http://www.ultratechnology.com/chips.htm>

In all, though, you're right. In this business, the elegance of
yore tends
not to remain in vogue.

REVIEW: "Digital Signatures", Mohan Atreya et al.

Rob Slade <rslade@sprint.ca>
Tue, 2 Jul 2002 07:43:29 -0800

BKDIGSIG.RVW 20020520

"Digital Signatures", Mohan Atreya et al., 2002, 0-07-219482-0, U
\$59.99

%A Mohan Atreya
%A Benjamin Hammond
%A Stephen Paine
%A Paul Starrett
%A Stephen Wu
%C 300 Water Street, Whitby, Ontario L1N 9B6
%D 2002
%G 0-07-219482-0
%I McGraw-Hill Ryerson/Osborne
%O U\$59.99 905-430-5000 +1-905-430-5134 fax: 905-430-5020
%P 368 p.
%T "Digital Signatures"

Although cryptography is generally considered to be useful for hiding information or holding it confidential, cryptographic methods can also be used to determine whether data has been altered. Slightly more specialized means can also be used to provide evidence that a certain individual composed or verified a certain message, in the same way that a handwritten signature is presumed to assert a person's intent or agreement with respect to a contract. Properly used and supported, these digital signatures can be stronger and more flexible than physical signatures as a means of binding an identity to a document.

Chapter one is an introduction, both to some basic concepts, and to the book

as a whole. (The material is disjointed in places: there is a section entitled "Legislation" on page six and another on page eight, although the content is different.) The overview of cryptography, in chapter two, has some very weak and some very good points: the explanation of the four modes of DES (Data Encryption Standard) is much clearer than in most texts. The description is, however, very generic, and does not address hash or signature topics at all, nor does it address algorithmic and key length strength and weakness. Certificates are a vital part of the common digital signature structure, but chapter three's discussion concentrates on X.509 fields and request procedures, without getting into the underlying concepts. Data integrity is another key (sorry) concept in the creation of digital signatures, but while the material on checksums and hashing starts out well, chapter four ends in something of a confusing mess. Chapter five flits between real and theoretical systems in such a way that no valid assessment of uses and shortcomings is possible. A number of miscellaneous topics are listed in chapter six. Chapter seven looks at various business issues and models, generally with respect to public key infrastructure, but is oddly unhelpful in real world terms. Some standards are listed and tersely described in chapter eight. Definition sections lifted from various pieces of legislation are reproduced in chapter nine. Chapter ten lists a number of legal concepts that may have a bearing on digital signatures: these are more practically related to systems and policies in chapter

eleven.

The technical and practical aspects of this book fall far short of being useful either to the security professional, or to the manager who may need to address the topic or make decisions about systems. The legal sections, however, might justify, for the professional, the purchase of this otherwise confused work.

copyright Robert M. Slade, 2002 BKDIGSIG.RVW 20020520
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

<http://victoria.tc.ca/techrev/~rslade> or <http://sun.soci.niu.edu/~rslade>



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

[ACM](#) Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 16

Sunday 21 July 2002

Contents

- [U.S. House approves life sentences for crackers](#)
[NewsScan](#)
- [Expert says Palm Beach's new voting machines have problems](#)
[PGN](#)
- [Palm Beach voters at it again](#)
[Dan Scherer](#)
- ['Face testing' at Logan is found lacking](#)
[Monty Solomon](#)
- [Japanese service links ATMs to cell phones](#)
[Mich Kabay](#)
- [Yahoo admits changing e-mail text to block hackers](#)
[Monty Solomon](#)
- [IIS Mail exploit](#)
[Matthew Byng-Maddick](#)
- [E-mail content filtering may kill the medium](#)
[Derek K. Miller](#)
- ["You may not have received this e-mail"](#)
[Monty Solomon](#)
- [Forensic programming course outline](#)
[Rob Slade](#)

- [Re: EULA](#)
[Derek J. Balling](#)
 - [REVIEW: "The Hacker Diaries", Dan Verton](#)
[Rob Slade](#)
 - [REVIEW: "Hacker Attack", Richard Mansfield](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ U.S. House approves life sentences for crackers

"NewsScan" <newsscan@newsscan.com>

Tue, 16 Jul 2002 09:18:43 -0700

The U.S. House of Representatives has approved the Cyber Security Enhancement Act (CSEA) by a near-unanimous vote [385-3]. Among the Act's provisions are an expansion of police ability to conduct Internet or telephone eavesdropping without first obtaining a court order, and the approval of life prison sentences for malicious computer hackers (crackers) whose acts "recklessly" put others' lives at risk. In the case of wiretaps, the Act would permit limited surveillance without a court order when there is an "ongoing attack" on an Internet-connected computer or "an immediate threat to a national security interest." The surveillance would be limited to collecting a suspect's telephone number, IP address, URLs or e-mail header information -- not the content of an e-mail message or phone conversation. In addition, the Act would permit ISPs to disclose the contents of e-mail messages and other electronic records to police in cases

when "an emergency involving danger or death or serious physical injury to any person requires disclosure of the information without delay." The Act is not expected to meet any serious opposition in the Senate. [CNet News.com

15 Jul 2002; NewsScan Daily, 16 July 2002]

http://news.com.com/2100-1001-944057.html?tag=fd_top

[Declan McCullagh notes that the CSEA had been written before 11 Sep 2001. PGN]

✶ Expert says Palm Beach's new voting machines have problems

Peter G Neumann <Neumann@CSL.sri.com>

Wed, 17 Jul 2002 00:34:50 -0400

Associated Press item by Jill Barton, 16 Jul 2002

The voting machines that replaced butterfly ballots and hanging chads are checked by an "Enron-style of auditing" and don't provide voters any assurance that their votes are being cast, an expert testified Tuesday.

Rebecca Mercuri, a computer science professor at Bryn Mawr College in

Pennsylvania, said questions remain about the \$14 million machines Palm

Beach County purchased to improve its voting system because they are

designed to audit themselves. "The problem with the self-auditing machines

is if it's broken, how can it tell you that it's broken?" Mercuri said.

Mercuri's testimony provided the latest criticism of a county

still

embarrassed by the 2000 election debacle. She was called in a Tuesday afternoon hearing to bolster a Boca Raton man's claims that he lost a City Council election in March because the new machines malfunctioned.

Former Mayor Emil Danciu's suit seeks to have the results overturned and a new election held. The suit includes affidavits from eight voters who said they had trouble casting ballots on the ATM-style machines and says voters should be given paper receipts to confirm their vote was recorded. It also seeks to allow an independent review of the voting machines and related software and security features.

Supervisor of Elections Theresa LePore says such a review would void the machines' warranty and that they've been reviewed twice by labs appointed by the federal government and also by a state worker. She says most of the information the plaintiffs are seeking is filed with the state Division of Elections in Tallahassee and even if it were available, she couldn't provide it because it includes trade secrets of Sequoia Voting Systems Inc., which manufactures the machines. "I'm not willing to let anyone take a machine and take it apart," LePore said. "I don't think the taxpayers would appreciate them taking apart a \$3,500 machine and voiding the warranty." LePore has said the only problems reported to her office following the March election were screens temporarily freezing when voters chose between English and Spanish, which did not prevent voting. She said the machines further

demonstrated that they work Saturday when the county held a mock election in supermarkets and shopping malls allowing voters to try out the machines.

✶ Palm Beach voters at it again

"Dan Scherer" <dans@oz.net>

Sat, 20 Jul 2002 11:43:35 -0700

As noted in an AP news article

<http://ap.tbo.com/ap/florida/MGAIFTWBQ3D.html>

and reviewed on /.

<http://slashdot.org/articles/02/07/20/0124232.shtml?tid=126>

some West Palm County voters and politicians are upset that their new "ATM style" voting machines have an internal auditing system that doesn't allow access to the "self-auditing" side of the software. Voters are claiming that the machine didn't register their votes, and that an election hangs in the balance because of the discrepancies.

The Slashdot crowd is holding this up as an example of where open source needs to be used while the equipment manufacturer refuses to disclose their trade secrets on the "self auditing" software.

The RISKS are obvious.

✶ 'Face testing' at Logan is found lacking

Monty Solomon <monty@roscom.com>

Wed, 17 Jul 2002 23:08:15 -0400

A test at Boston's Logan International Airport has found that computerized facial-recognition systems, one of the most trumpeted new technologies in the war on terrorism, may not be a practical tool for airport security. The machines were fooled when passengers turned their heads in certain directions, and screeners became overtaxed by the burdens of having to check passengers against a large pool of faces that closely resemble theirs.

Hiawatha Bray, **The Boston Globe**, 17 Jul 2002.

[http://www.boston.com/dailyglobe2/198/metro/
Face_testing_at_Logan_is_found_lacking+.shtml](http://www.boston.com/dailyglobe2/198/metro/Face_testing_at_Logan_is_found_lacking+.shtml)

⚡ Japanese service links ATMs to cell phones

Mich Kabay <mkabay@compuserve.com>

Wed, 17 Jul 2002 18:56:07 -0400

NTT DoCoMo is set to launch the world's first service that enables cell phone users to withdraw cash from automated teller machines located in convenience stores and supermarkets. Instead of inserting a bank card into the designated slot, users of DoCoMo's 504i handsets would push a few buttons on their phones in order to complete an ATM transaction. Analysts said the system was certainly novel, but it's still unclear how user-friendly it will prove. "Younger people may be more receptive, but

people generally already have cash cards," says an analyst at a foreign securities firm. DoCoMo says the new system, which it is offering in partnership with IY Bank, likely will launch sometime in early 2003.
(Reuters/Yahoo, 16 July 2002)

http://story.news.yahoo.com/news?tmpl=story2&cid=581&ncid=581&e=9&u=/nm/20020716/tc_nm/financial_japan_iybank_dc_2

I think no comment is necessary on the RISKS of linking banking systems to wireless phone systems. It will be worth watching developments.

M. E. Kabay, PhD, CISSP, Dept CompInfoSys, Norwich University, Northfield VT

<http://www2.norwich.edu/mkabay/index.htm>

Yahoo admits changing e-mail text to block hackers

Monty Solomon <monty@roscom.com>

Wed, 17 Jul 2002 23:09:10 -0400

... Yahoo! Inc. has confirmed that its e-mail software automatically changes certain words -- including "evaluate" -- in a bid to prevent hackers from spreading viruses. Although the company declined to list the words its software had been changing, a report on the technology news Web site, News.com, reported that the program changes "mocha" to "espresso," and the phrase "eval" to "review." [Article by Andrea Orr, Reuters, 17 Jul, 2002, noting that your applications for employment may have been

altered! PGN]

<http://finance.lycos.com/home/news/story.asp?story=27883602>

✶ IIS Mail exploit

Matthew Byng-Maddick <mbm@colondot.net>

Sun, 14 Jul 2002 23:50:55 +0100

The recent IIS Mail encoding bug has not yet made it into RISKS. The bug in question was an encoding error in the mail component of IIS, but unlike a lot of the other encoding bugs in IIS, which, as far as I understand it, only allow the server in question to be compromised, this bug makes the server into an open relay. What's the difference, you may ask. Spammers have been looking at exploiting mail relays for some time in an effort to avoid some of the audit trail used in the message (the Received: headers, inserted by the MTAs), they've tried with buffer overflows and other such things. Now they suddenly have a trivial way of trying to relay a message. Of course, all that will happen is that the test should get added to a half of the current Open Relay Blacklists (ordb, orbz etc.), but then we risk blackholing a fair amount of the Internet, because, like it or not, large numbers of Microsoft servers are appearing and being used.

When will it all stop?

Matthew Byng-Maddick <mbm@colondot.net> <http://colondot.net/>

✶ E-mail content filtering may kill the medium

"Derek K. Miller" <dkmiller@pobox.com>

Wed, 17 Jul 2002 12:48:18 -0700

E-mail filtering, in an effort to stop spam, has become insidious. Used properly -- especially by individual users -- it can be quite helpful. Used sloppily to filter for semi-arbitrary spamlike content (as it often is by server administrators and others), it risks killing e-mail as a useful form of communication.

I'd highly recommend the following articles and discussion at the TidBITS mailing list site, which cover the issue and its hazards in clear and useful detail:

Killing the Killer App

<http://db.tidbits.com/getbits.acgi?tbart=06866>

Content Filtering Exposed

<http://db.tidbits.com/getbits.acgi?tbart=06869>

Various discussion threads:

<http://db.tidbits.com/getbits.acgi?tlkthrd=1679>

<http://db.tidbits.com/getbits.acgi?tlkthrd=1680>

<http://db.tidbits.com/getbits.acgi?tlkthrd=1681>

<http://db.tidbits.com/getbits.acgi?tlkthrd=1683>

<http://db.tidbits.com/getbits.acgi?tlkthrd=1684>

Here's a pertinent excerpt:

```
> * Email is increasingly being filtered for its content;  
>
```

> * That filtering is often being done without the knowledge or
> consent of affected users;
>
> * Over time, inaccurate filtering will substantially reduce
> the general utility of email.
>
> In short, we're starting to see signs that email, often hailed
> as the Internet's "killer app," is in danger of becoming an
> unreliable, arbitrarily censored medium - and there's very
little
> we can do about it.

Derek K. Miller, Vancouver, BC, Canada dkmiller@pobox.com
<http://www.penmachine.com>

✶ "You may not have received this e-mail"

Monty Solomon <monty@roscom.com>
Wed, 17 Jul 2002 23:10:26 -0400

Web Informant #293, 9 July 2002:
You may not have received this e-mail

George Carlin once had a bit about the seven dirty words that
couldn't be
said on TV: if only our email systems were as discrete and
predictable about
the nature of their censorship. Indeed, I can almost guarantee
that if I
include certain words in this message (such as viag--, -orn,
make -oney
-ast, or any of Carlin's seven choice words), many of you won't
ever get
this email.

The trouble is that spammers, virus authors (or whatever
deriding term you
would like to use to call the scum that create these

annoyances), and others have become too clever at creating their garbage. And in the ever escalating war of technology, email filtering products have become too good at cutting off legitimate messages, just because they contain the equivalent of Carlin's list.

The best research on this was an article that was posted to the TidBITS mailing list this past week. If you are interested in Macs and in general the Internet, this is a weekly series of essays that Adam Engst and other write and distribute for free via e-mail to over 40,000 people, along with posting it to tidbits.com and many other web sites. Geoff Duncan concludes several trends:

<http://strom.com/awards/293.html>

✶ Forensic programming course outline

Rob Slade <rslade@sprint.ca>
Sun, 21 Jul 2002 14:15:51 -0800

I am currently teaching forensic programming, at roughly the third-year college/university level, at BCIT, and the course will also be run in the fall and again in the spring. Since this is the first course of its kind (as far as I have been able to determine), and since most of the resources (somewhat by necessity) are online, I am beginning to put together the

course outline and resources as a set of Web pages. This is not
(so far)
anything like a full online course: for one thing, I have not
(so far)
written out complete lecture notes. However, for those
interested, the
"table of contents" page is available at
<http://victoria.tc.ca/techrev/fptoc.htm> or
<http://sun.soci.niu.edu/~rslade/fptoc.htm> (and also
<http://cstbtech.bcit.ca/FP/index.html>).

This is very much a work in progress, and will be updated and
expanded
frequently in the coming weeks.

rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

<http://victoria.tc.ca/techrev> or [http://sun.soci.niu.edu/
~rslade](http://sun.soci.niu.edu/~rslade)

✉ Re: EULA

"Derek J. Balling" <dredd@megacity.org>

Mon, 15 Jul 2002 10:58:08 -0400

Something which occurred to me, working in the healthcare
industry
these days, is that I'm not sure - given HIPAA compliancy
regulations
and the like - that I *can* agree to allow companies permission
"to
install random software on random machines without any notice or
confirmation".

As security concerns, especially in terms of personal
information protection
and such, get more and more codified into law, the chance that a
business

will run afoul of the "Choose between obeying the law and obeying the EULA" dilemma are going to be on the increase. Given certain Pacific Northwest companies' love for deep-pockets litigation to enforce EULA's after the fact, whichever choice is made is certain to be costly in one manner or another.

I've already pointed out to the head our IT department that from my cursory, non-lawyer, reading of the WinXP EULA, we have to move it from the "we don't support this" category to the "this is explicitly forbidden from our machines" category.

Derek J. Balling <dredd@megacity.org> www.megacity.org/blog/

REVIEW: "The Hacker Diaries", Dan Verton

Rob Slade <rslade@sprint.ca>
Mon, 15 Jul 2002 07:59:32 -0800

BKHCKDRY.RVW 20020519

"The Hacker Diaries", Dan Verton, 2002, 0-07-222364-2, U\$24.99
%A Dan Verton
%C 300 Water Street, Whitby, Ontario L1N 9B6
%D 2002
%G 0-07-222364-2
%I McGraw-Hill Ryerson/Osborne
%O U\$24.99 905-430-5000 +1-800-565-5758 fax: 905-430-5020
%P 219 p.
%T "The Hacker Diaries: Confessions of Teenage Hackers"

Teenaged hackers are misunderstood. Definitions are for lamers, morality is a "bogus" concept. These noble idealists are

questers

after the Holy Grail of knowledge: problem solvers who are attempting

to enlighten the masses. Given a little dedication, you too can, inside of six months, go from being a technopeasant to "knowing everything there [is] to know" about computers. Thus it is written in the Gospel of Verton.

(While we are at it, I have this nice bridge you might want to purchase ...)

Even if you ignore questions about the definition of what "hacking" actually

is, and even if you leave aside the author's biased sympathy for rebels-without-a-clue, the introduction alone points out that Verton has not

performed the research one would think minimal to such a project: reading

the "popular" literature on the subject, never mind the more serious

analyses by researchers like Denning and Gordon. How else can he make the

statement that this book is the first ever to try and penetrate the veil of

secrecy surrounding the computer vandal community, an assertion that must

come as a bit of a shock to authors like Levy ("Hackers," cf. BKHACKRS.RVW),

Sterling ("Hacker Crackdown," cf. BKHKRCRK.RVW), Taylor ("Hackers,"

cf. BKHAKERS.RVW), Dreyfus ("Underground," cf. BKNDRGND.RVW), and a host of

others. It is, therefore, no surprise that this author gets basic factual

information wrong, such as the confusion of the infamous Operation Sundevil

with more successful prosecutions of computer crime.

Verton decries the blind and ignorant stereotyping of loners who are more

comfortable with computers than with their peers, but he is, himself, guilty

of promoting the same kind of confusion. The group targeted after the Columbine shootings was not the computer community but the Goths, who share almost no characteristics with hackers except for a slightly obsessive interest in an esoteric topic and a position outside the mainstream. (Well, possibly also an aversion to sunlight ...) Verton has attempted to include "representative" examples of both maladjusted criminals and ethical hackers, but draws no distinctions between them and, indeed, seems to be trying to lump them all together.

No, I've changed my mind. Let's not leave aside the question of a definition of hacking. Like too many authors, Verton also wants to continue the confusion of the original idea of a hacker as a skilled technologist with the more recent concept of the vandals of computer systems. But he also immediately destroys his position by pointing out that a cracker cannot change his "handle," the (usually offensive) nickname used to achieve both identity and anonymity online. If an underground "hacker" changes his handle, he loses his status and becomes just another wannabe. Verton does not seem to realize the import of this statement. A cracker's credibility is tied to his nickname, since he is only as good as his "rep," the record of defacements or intrusions he is able to boast about. There is no actual skill set behind such a reputation. In opposition, if true hackers like Richard Stallman or Eric Raymond were to change their names, and were then to write new programs and release them to the world, those

programs would still be useful and of good quality. (Top programmers would, in fact, probably be able to identify the authors of emacs and fetchmail by programming excellence and style.)

Verton's writing seems clear and readable unless you start to think about it. A story will say that A happened, then B happened, then C happened, then B happened, then D happened, then B happened. Times are quite indefinite, but since the narrative is unclear even about simple sequences it is not any real shock to find out that the author does not know larger items of technical history, such as that UNIX predates VMS. Likewise, Verton isn't interested in having consistency get in the way of a good story, even if the story doesn't make any sense. Directions and motivations change suddenly and without apparent reason: reading between the lines indicates that there is a lot that we aren't being told. Probably the author wasn't told, either. It sounds like he didn't even ask. (The interview subjects seem to have realized that they were dealing with a credulous author: Verton retails stories out of common urban legends and jokes without seeming to have identified them as such. Despite his credentials as a reporter for a computer trade magazine Verton's technical knowledge is questionable--he doesn't know a denial of service attack from a reformat nor that the Macintosh doesn't have a Windows Registry.)

Despite tidbits of trivia, ultimately the book is boring. One can only read

so many times that Amanda (or Betty or Cathy) accidentally touched a computer on her seventh birthday and thereafter became obsessed with re-writing the CP/M kernel before one loses interest. The names may change, the hacks may change, the outcomes and choices of whether or not to be useful or messed up may change, but in the end, the lessons are the same: non-existent.

copyright Robert M. Slade, 2002 BKHCKDRY.RVW 20020519
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

<http://victoria.tc.ca/techrev/~rslade> or <http://sun.soci.niu.edu/~rslade>

REVIEW: "Hacker Attack", Richard Mansfield

Rob Slade <rslade@sprint.ca>
Thu, 18 Jul 2002 15:30:41 -0800

BKHCKATK.RVW 20020519

"Hacker Attack", Richard Mansfield, 2000, 0-7821-2830-0,
U\$29.99/C\$44.95/UK#19.99

%A Richard Mansfield earth@worldnet.att.net

%C 1151 Marina Village Parkway, Alameda, CA 94501

%D 2000

%G 0-7821-2830-0

%I Sybex Computer Books

%O U\$29.99/C\$44.95/UK#19.99 510-523-8233 Fax: 510-523-2373

%P 293 p.

%T "Hacker Attack: Shield Your Computer from Internet Crime"

"FACT: It's unlikely that you'll ever personally experience a computer

virus in your home computer." Ah, those glowing, carefree days of yore when ... wait a minute. This book wasn't published all THAT long ago ...

This work is intended to address three issues: intrusions, privacy, and viruses. The author hopes that it will be as much fun to read as it was to write. Given the unrealistic assessment of risk levels, the almost random choice of topics, and the lighthearted approach, I did not start out feeling confident of the chances of finding useful information herein.

(While we may agree that script kiddies and such cracker wannabes are grubs and insects, the security community does **not** refer to them as "larvae.")

Part one is entitled "Hackers, Crackers, and Whackers." Chapter one is a generic warning about the fact that some people may be trying to probe you. Some information (such as directions on turning file and print sharing off) are useful, others (such as the need to share IP addresses--assuming you even know them--with friends for chatting and instant messages) are either wrong or not very useful. Port scanning gets mentioned, and, aside from the fact that there are more reliable ways of determining open ports, the specific example of an open port used isn't terribly handy since we are told neither what it is nor how to turn it off. Phone phreaks are discussed in chapter two--without mention of the fact that in-band signalling is now

obsolete. Hackers are academics studying decryption, viruses can harvest your passwords, and munging your e-mail address is an effective tool against spam, or so we are told in chapter three. Chapter four gives names to some really silly cracking techniques. Some equally silly defences are suggested in chapter five. Chapter six does say that there are better protections available, but doesn't talk about how to implement them. High-speed connections are said to be security risks (the real culprit being static IP addresses) in chapter seven. A variety of URLs are given for the ZoneAlarm product, and instructions for getting warnings about cookies from one version of the Internet Explorer browser are provided in chapter eight.

Part two is supposed to deal with privacy. Chapter nine does, with a rapid race through a number of related issues. Chapters ten through thirteen, however, examine a number of encryption technologies that are no longer used. The algorithm central to DES (Data Encryption Standard) is used as an example of a symmetric encryption system in chapter fourteen. Chapter fifteen explains the use of prime numbers to create asymmetric (public key) systems. Both of these chapters are remarkably unhelpful in terms of the actual use of encryption. Chapter sixteen explains digital signatures, but very briefly. The dialogue boxes involved in using the Encrypting File System of Windows 2000 are displayed in chapter seventeen. Chapter eighteen speculates on quantum computers. Source code for a random number generator

for a
one-time pad is given in chapter nineteen.

Part three looks at viruses. (Ready?) Chapter twenty gives a
brief
account of the Internet/Morris/UNIX Worm of 1988, informing us
that
viruses had been used for years for network administration
(untrue)
and failing to explain what defrauding your girlfriend has to do
with
the worm. Some basics of virus structure are correct in chapter
twenty one, but there is also confusion of pranks and trojans,
and the
discussion of virus functions applies only to boot sector
infectors.
Chapter twenty two provides an overview of Melissa and
Loveletter.
Useless means of defending against Microsoft Word macro viruses
(known
to have been bypassed long before this book was written) are
given in
chapter twenty three. Chapter twenty four tells us that viruses
are
mainly hype.

Well, there are a few tips in this work that might help you to
prevent
intrusions, protect your privacy, and avoid viruses. Very few.
The
material is scant, and is padded out to book length with random
insertions only nominally related to the topics at hand.
Although not
stated, it is fairly clear that the volume is intended for the
average
computer user rather than the security specialist. In terms of
that
general audience, the text is nowhere near detailed enough in
those
areas that the typical user can address. The material on network
intrusions has some points, but many gaps. The section on
cryptography might be interesting to a few, but is of little
practical

use. The opining on viruses is too often flatly wrong.

copyright Robert M. Slade, 2002 BKHCKATK.RVW 20020519
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

<http://victoria.tc.ca/techrev~rslade> or <http://sun.soci.niu.edu/~rslade>



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 17

Wednesday 24 July 2002

Contents

- [Warning system failed during fatal tornado](#)
[Robert Crump](#)
- [Wrong number costs Gateway \\$3.6 million](#)
[NewsScan](#)
- [WebTV virus dials 911](#)
[Monty Solomon](#)
- [Explanation of Voter-Verified Ballot Systems](#)
[Rebecca Mercuri](#)
- [Auditing of voting machines](#)
[Daniel Boyd](#)
- [Royalty fees may be the death of Internet radio](#)
[NewsScan](#)
- [SSH Protocol Weakness Advisory](#)
[Monty Solomon](#)
- [Uselessness of "Dirty word" filters](#)
[Danny Lawrence](#)
- [E-mail content filtering may kill the medium](#)
[Pascal Bourguignon](#)
[Max TenEyck Woodbury](#)
- [Yahoo! *fixes* e-mail as security measure](#)

[Robert Gezelter](#)

● [Re: Crackers -- aka hackers -- providing useful information](#)

[Fred Gilham](#)

● [Doonesbury, Allen Hutchinson on 802.11 networks and security](#)

[Declan McCullagh](#)

● [Monty Solomon <monty@roscom.com>](#)

● [Setuid Demystified, Chen/Wagner/Dean](#)

● [11th USENIX Security Symposium](#)

[Alex Walker](#)

● [REVIEW: "Writing Information Security Policies", Scott Barman](#)

[Rob Slade](#)

● [Info on RISKS \(comp.risks\)](#)

⚡ Warning system failed during fatal tornado

Robert Crump <rwcrump@comcast.net>

Tue, 23 Jul 2002 23:18:42 -0400

Subtitle: Glitch kept radio station from relaying storm alert
Associated Press, in the **Baltimore Sun**, 23 Jul 2002

According to the National Weather Service, an Emergency Alert System designed to enable WTOP in Washington DC to forward warnings of dangerous weather conditions to small radio stations in up to 28 counties failed on 28 Apr 2002, just before a deadly tornado struck Southern Maryland. The warning was intended for 31 DC-area counties, more than the system was programmed to accommodate. The storm spawned a strong tornado that cut through Southern Maryland, causing five deaths, an estimated \$120 million in damage and destroying much of downtown La Plata.
[PGN-ed]

✦ Wrong number costs Gateway \$3.6 million

"NewsScan" <newsscan@newsscan.com>

Mon, 22 Jul 2002 08:41:48 -0700

A federal court has awarded a Pensacola business \$3.6 million in damages from Gateway, which had accidentally distributed the wrong phone number for customer complaints to more than 275 Gateway stores. The error dated back to 1999, when someone at Gateway erred by using the 800 prefix instead of the correct 888 prefix for the company's toll-free customer complaint line. The wrong number was also posted on Gateway's Web site, listed on Internet billings and included on a form distributed to more than 100,000 Gateway customers. Mo' Money, which manufactures and distributes promotional items, said it contacted Gateway six days after the calls began, but that it took the computer company more than two years to fix the problem. "It was a nightmare," says Mo' Money president Cliff Mowe. "We had as many as 8,000 extra calls a month, and these were all angry people You couldn't get them off the line because the only number they had was ours. You'd have to explain it and go through it, and a lot of times they'd call you right back anyway." [Associated Press, 19 Jul 2002; NewsScan Daily, 20 July 2002]

<http://apnews.excite.com/article/20020719/D7KS83F82.html>

⚡ WebTV virus dials 911

Monty Solomon <monty@roscom.com>

Tue, 23 Jul 2002 19:45:01 -0400

Police show up only to find infected WebTVs.

A new virus has hit some WebTV devices, and its effects could have ramifications for the emergency phone network. Reportedly, once an attachment is opened using the WebTV set-top box, the virus dials 911. A customer service supervisor at Microsoft confirms that 18 customers have called in to report the suspicious WebTV behavior. WebTVs now go by the name MSNTV, but older brands still have the WebTV branding. According to Microsoft, both units are affected.

<http://www.techtv.com/news/security/story/0,24195,3392631,00.html>

[PGN adds: see also

http://www.abcnews.go.com/sections/scitech/TechTV/techtv_911virus020723.html

]

⚡ Explanation of Voter-Verified Ballot Systems

"Rebecca Mercuri" <notable@mindspring.com>

Wed, 24 Jul 2002 15:54:47 -0400

An explanation of the necessity for a

Voter Verified Physical Audit Trail for Electronic Balloting Systems

by Rebecca Mercuri, Ph.D.

Professor of Computer Science at Bryn Mawr College

Electronic voting info: <http://www.notablessoftware.com/evote.html>

Email: mercuri@acm.org

Phone: 609/895-1375, 215/327-7105

Many of the new voting products now being purchased in the US are self-auditing in that they produce ONLY an internal electronic audit of the ballots cast. Some of these machines have been sold with trade secret protection such that it is not possible to INDEPENDENTLY examine the machines for correct operations (except perhaps under court order, and even there the examination may be required to be sealed or not disclosed).

This situation, which is becoming more common as fully-electronic (DRE/kiosk) voting systems are introduced, means that the voters as well as the poll workers and election officials have NO WAY to verify that their ballots are recorded, transmitted and tabulated properly. Machines have failed in actual use and independent recounts have not been provided. (See reports in press accounts.)

Some systems re-create a set of ballots, on paper, AFTER the election, which is presented for recount purposes. Since this set of ballots is self-generated, errors in the equipment may be reflected in the self-audit, with the appearance of being correct. There is no way to determine whether this after-the-fact paper reflects the true contents of the ballots cast. Only if the voter has the opportunity to review the paper generated at the time of voting, that will be used in the recount, is an

independent

audit possible. In the same way, if the system is used to self-report its stored ballots, its true error rate can not be ascertained.

It is essential, therefore, that voters be able to create a physical or paper ballot that is deposited at the polling place when their vote is cast. This ballot, which can be scanned in or hand-counted since it is human-readable, would be used to verify any machine-generated tallies produced from electronic (DRE) voting systems. Only in this way can the voters be assured that their ballot will be available for an independent recount.

Congress is now in conference on the Voting Rights Act bills H. R. 3295 and S. 565. The Senate bill refers to "audit capacity" and "error rate" although the House bill does not mention these specifically. It is imperative that the compromise bill refer to a "physical audit capacity" or even more specifically a "voter verified independent physical audit capacity" (or audit trail) in order to prevent self-auditing systems from continuing to be accepted and used for elections in the United States.

Further explanation follows below:

All Direct Recording Electronic (DRE) voting systems must provide a physical audit trail that is reviewed by the voter at the time their ballot is cast.

(DRE voting systems are those that are constructed as to be self-contained, where the voter makes ballot choices that are directly entered

onto

electronic data recording devices. These would include stand-alone kiosks as well as networked machines.) The physical audit trail could consist of a printout that the voter can examine independent of any computerized display.

If a voter determines, at the time of balloting, that the printout does not reflect the votes they just cast on the machine, there must be a procedure where the electronic and paper ballot can both be voided and another opportunity to vote allowed. The reviewed and accepted printout would be deposited into a ballot box for subsequent optical scanning or hand-counting in order to produce the true results for the election. Totals provided by the DRE devices can be used to provide early returns, but the final result (in case of dispute) should be determined from the paper ballot set. The voter-verified physical ballots must be those which are used and preserved as the permanent audit trail for the election.

Since it is, in principle, impossible to verify that a computational device is free from programming errors or nefarious code, no electronic voting system can be verified for 100% accuracy, reliability, and integrity. It is also, in principle, impossible for a computational device to provide full fail-safe internal verification, hence any ballot audit produced from self-stored data could reflect errors or manipulation that occurred between the time the voter cast their ballot and the time the ballot was recorded.

Errors and manipulation of ballots can also occur if data is transmitted

between devices or over networks. It is essential, therefore, that each voter provide an independent check of their ballot at the time of voting, using human-readable media as the manual audit capacity for the voting system.

Confidence in the electronic recording devices can be assured only if the voters have an independent way of verifying that their ballots were cast and submitted for counting (and re-counting) as intended.

✶ Auditing of voting machines

Daniel Boyd <boyd@buffalo.edu>

22 Jul 2002 14:20:03 -0000

It strikes me that the auditing of the Palm Beach electronic voting machines doesn't even reach the level of care applied to Las Vegas slot machines.

Slot machines are governed by a Nevada state agency and are continually inspected at random. The inspectors pull a machine out of service, check that the circuit boards are the correct, legally-certified boards that are supposed to be in the machine, and read the PROMs. The state has enough access, and knowledge of the design, to verify not only the program that is supposed to be running on the hardware, but the hardware itself.

That "proprietary-hardware/trade-secrets" excuse wouldn't get one of those Palm Beach machines within ten feet of a casino floor in Nevada.

✶ Royalty fees may be the death of Internet radio

"NewsScan" <newsscan@newsscan.com>

Mon, 22 Jul 2002 08:41:48 -0700

All kinds of radio stations -- both Web-based and traditional over-the-air broadcasting stations -- have to pay copyright royalties to songwriter associations, but only the Web stations are required to pay a new performer's fee that goes to record companies. At a rate of seven-hundredths of a cent per song per listener, the fee is expected to undo the economic viability of almost all of the 10,000 Web radio stations now in existence.

The 200 stations that have already ceased operations include nonprofit stations at UCLA, NYU, and other colleges and universities, and people seem to be punching different calculators to attack or defend what's going on:

Congressman Rick Boucher (D, VA) is introducing a bill in support of small

Webcasters and says its goal is "to make sure that Webcasters who measure

their revenues in the tens of thousands are not put out of business by a

copyright payment requirement in the hundreds of thousands." ; using a

different calculator, Hilary Rosen of the Recording Industry Association of

America (RIAA) says that most college stations won't owe more than \$500 a

year, and adds, "Given our problems with digital piracy on university

servers, it is almost comical that they have the nerve to

complain about

\$500." [**USA Today**, 21 Jul 2002; NewsScan Daily, 20 July 2002]

http://www.usatoday.com/tech/news/techpolicy/2002-07-21-radio_x.htm

SSH Protocol Weakness Advisory

Monty Solomon <monty@roscom.com>

Tue, 23 Jul 2002 19:14:15 -0400

<http://online.securityfocus.com/archive/1/283688>

Cuts like a knife, SSHarp

<http://www.phrack.org/show.php?p=59&a=11>

SSH for fun and profit

<http://segfault.net/~stealth/ssharp.pdf>

Uselessness of "Dirty word" filters

"Danny Lawrence" <Danny@TiassaTech.com>

Mon, 22 Jul 2002 11:20:16 -0400

As a horse-racing fan, there are a couple of WWW based message boards that I post to. Some of these have "Dirty word" filters, on one of which each mention of the horse Dr. Fager (the only horse to win Eclipse "Horse of the year" awards in 4 different categories in one year) got rejected by the DW filter. Why, you ask? It took me a while to figure out but the DW filter

was treating the the horse's name as "<derogatory term>" + "er"!

Danny Lawrence, Tiassa Technologies Inc., A Lotus Business Partner

[Long ago, horse's names were restricted to something like 13 characters,

because of technical restrictions on old-style tote-boards. Perhaps now

we will next see horse-name restrictions that ban certain undesirable

substrings. And perhaps other sports will ban players with offensive

names -- unless those players are willing to change their names. PGN]

✂ E-mail content filtering may kill the medium (Miller, [RISKS-22.16](#))

Pascal Bourguignon <pjb@informatimago.com>

Mon, 22 Jul 2002 08:20:36 +0200 (CEST)

There's a very little step we can do to very effectively fight this and many other problems: just use PGP.

* Just PGP signing an e-mail is enough to ensure that the e-mail content is not altered without notice.

* Just PGP encrypting is enough to ensure that the e-mail content cannot be filtered.

Pascal_Bourguignon <http://www.informatimago.com/>

[PGP SIGNATURE deleted by PGN, as is his custom for RISKS.]

✶ Re: E-mail content filtering may kill the medium (Miller, [RISKS-22.16](#))

Max TenEyck Woodbury <mtew@cds.duke.edu>

Mon, 22 Jul 2002 14:58:18 -0400

Two questions need to be asked about this line of arguments:

- 1) What and how damage would result if e-mail was never filtered.
- 2) Do the opponents of this activity suffer some kind of financial loss when it is performed, and who gains, if anyone, when it happens.

As I understand it, the main purposes of the filters is to control the amount of unsolicited (usually commercial) bulk e-mail a.k.a. spam. I've seen reports that UBE is a significant contributor to network infrastructure costs, which accrue to the recipient, not the sender. The filters do seem to be having some positive (from the recipients point of view) impact on the spam problem.

Some sophistication may be needed when reading the headlines in the original posting. For example, is the 'Killer App' being killed personal e-mail, or spam? Are the 'affected users' the targeted recipients or the senders of the spam? Is that the 'general utility of e-mail' to the public at large or to the spammers that is being reduced? Is this the personal communication medium called e-mail or an advertising medium called e-mail being discussed?

There is a substantial risk here, but it may not be the obvious

one!

⚡ Yahoo! *fixes* e-mail as security measure (Re: Solomon, [RISKS-22.16](#))

Robert Gezelter <gezelter@rlgsc.com>

Mon, 22 Jul 2002 13:00:03 -0500

Note: Written completely based on "Some Serious Word-Scrambling at Yahoo"

The New York Times, 22 Jul 2002.

The risks of this kind of re-writing are many, and the potential damage cannot be easily quantified. As the article notes, it can be humorous (when rewriting foreign languages such as French) to the more serious, to wit:

- a rewritten message might trigger another filter in a non-obvious way
(e.g. Carnivore, SPAM) possibly launching an uncalled for investigation
(a hazard mentioned in my March talk at E-Protectit; abstract and slides
at <http://www.rlgsc.com/e-protectit/sorcerers.html>);
- damage to business relationships (and the resulting legal exposures);
- damage to personal relationships.

There are numerous cases where micro-parsing of statements has caused much confusion (a hazard all too familiar to high-level diplomatic translators).

I do not want to prognosticate on issues such as responsibility,

but it seems that there is a substantial hazard of "friendly fire" damage in such cases.

In short, apparently the re-writes were not advertised and disclaimed, so who is responsible when damage occurs?

Robert "Bob" Gezelter, 35-20 167th Street, Suite 215, Flushing NY 11358-1731
+1 (718) 463 1079 <http://www.rlgsc.com> gezelter@rlgsc.com

✶ Re: Crackers -- aka hackers -- providing useful information

Fred Gilham <gilham@csl.sri.com>
Mon, 22 Jul 2002 10:50:02 -0700

Recently, while doing research on how to use the ELF (extensible linker format, or executable and linker format, depending on what you read) I discovered that the most useful information was put out by the cracker community. I found three papers that gave detailed information on how to use ELF features including example code. In one case, the intent was to allow 'parasites' to be embedded in a UNIX program; in another the author was exploring binary encryption as a means of preventing forensic analysis of an attack. In the third case, the paper described ways to allow a parasite to access shared library functions.

I'm not sure what to make of this. On the one hand, I don't want anyone

running `parasites' on my computers. On the other hand, this information saved me a lot of digging and experimentation.

Fred Gilham <gilham@csl.sri.com>

✶ Doonesbury, Allen Hutchinson on 802.11 networks and security

Declan McCullagh <declan@well.com>

Mon, 22 Jul 2002 00:58:07 -0400

This is hardly a new topic, but it's a good reminder. Also see Doonesbury, 21 Jul 2002 at <http://www.doonesbury.com>
-Declan

> Date: Sat, 20 Jul 2002 19:17:30 -0700
> From: "Allen Hutchison" <allen@hutchison.org>
> Subject: Watch your wireless configs...
>
> Last night I was playing around with the newest version of Lindows. I haven't worked with the OS much to date, because it didn't have support for my Cisco Aironet card. Since the card was the only way laptop can connect to the network I didn't want interrupt that ability. Anyway, yesterday a college of mine told me that Lindows now had support for wireless cards. So, I took the plunge and installed the OS on my laptop.
>
> The first thing I noticed, after the installation completed, was that my wireless card was blinking. I thought that the Lindows install had grabbed the settings for my card before it wiped windows off the machine. So I

> started trying to download software and access my network resources. Then I
> noticed that the network seemed really unresponsive. I started looking more
> closely at the network, and found that Linksys had not grabbed my previous
> settings, and I was associated with someone else's access point. To be sure
> I went to the default router address with a web browser, and found that it
> was a Linksys.
>
> Well, I thought, that isn't too strange, I have a Linksys on my network too.
> So I tried to log in, but it wouldn't take my password. So I tried the
> default password on a Linksys router "Admin" and I got in. Then I realized
> that I wasn't logged into my network at all. I was getting to the net
> through somebody else's access point somewhere else in the network.
>
> This person had never bothered to do anything to secure his network. Upon
> further inspection with a sniffer, I found that I could grab all of his
> traffic off the air in my office. He was using no encryption and no access
> control. I could browse the shares on his computer, I could see his password
> flying by. If I only knew where he lived, I could go tell him, and help him
> set up something more secure. All I know, however, is a general direction
> from my condo, South.
>
> This goes to show how important it is for vendors to stress security with
> their wireless products. Information is becoming more and more of a
> commodity, and the information that describes us is moving around on the

> Internet every day. When we install new technology, it is the
> responsibility
> of a vendor to explain the security consequences. It was
> obvious in the case
> of my mysterious neighbor that he hasn't installed any
> security on his
> network. It is quite possible he isn't even aware of the
> security hole he
> has opened onto his data.
>
> Something to think about.
>
> www.hutchison.org/allen
>
> FROM POLITECH -- Declan McCullagh's politics and technology
> mailing list
> You may redistribute this message freely if you include this
> notice.
> To subscribe to Politech: [http://www.politechbot.com/info/
subscribe.html](http://www.politechbot.com/info/subscribe.html)
> This message is archived at <http://www.politechbot.com/>

Setuid Demystified, Chen/Wagner/Dean

Monty Solomon <monty@roscom.com>

Tue, 23 Jul 2002 19:29:56 -0400

Setuid Demystified

Hao Chen, Computer Science Department, University of California
at Berkeley

David Wagner, Computer Science Department, University of
California at Berkeley

Drew Dean, Computer Science Laboratory, SRI International
Proceedings of the 11th USENIX Security Symposium, 5-9 Aug 2002
[see next item]

Abstract

Access control in Unix systems is mainly based on user IDs, yet the system calls that modify user IDs (uid-setting system calls), such as `setuid`, are poorly designed, in-sufficiently documented, and widely misunderstood and misused. This has caused many security vulnerabilities in application programs. We propose to make progress on the `setuid` mystery through two approaches. First, we study kernel sources and compare the semantics of the uid-setting system calls in three major Unix systems: Linux, Solaris, and FreeBSD. Second, we develop a formal model of user IDs as a Finite State Automaton (FSA) and develop new techniques for automatic construction of such models. We use the resulting FSA to uncover pitfalls in the Unix API of the uid-setting system calls, to identify differences in the semantics of these calls among various Unix systems, to detect inconsistency in the handling of user IDs within an OS kernel, and to check the proper usage of these calls in programs automatically. Finally, we provide general guidelines on the proper usage of the uid-setting system calls, and we propose a high-level API that is more comprehensible, usable, and portable than the usual Unix API.

<http://www.cs.berkeley.edu/~daw/papers/setuid-usenix02.pdf>

[Nifty paper. PGN]

11th USENIX Security Symposium

Alex Walker <alex@usenix.org>

Tue, 23 Jul 2002 10:44:48 -0700

There's still time to register for 11th USENIX Security Symposium being held 5-9 Aug 2002 in San Francisco. Check out <http://www.usenix.org/sec02> for detailed information and to register. This year's Symposium features the most recent developments in vb and network security. Keynote speakers Whitfield Diffie & Howard Schmidt, free vendor exhibition, the latest Research in OS Security, Access control, Hacks/Attacks, Web Security, Sandboxing, Deploying Crypto, and much more.

Alex Walker, Production Editor, USENIX Association
2560 Ninth Street, Suite 215, Berkeley, CA 94710 1-510-528-8649
x33

REVIEW: "Writing Information Security Policies", Scott Barman

Rob Slade <rslade@sprint.ca>

Mon, 22 Jul 2002 08:00:12 -0800

BKWRINSP.RVW 20020601

"Writing Information Security Policies", Scott Barman, 2002,
1-57870-264-X, U\$34.99/C\$52.95/UK#27.50

%A Scott Barman scott@barman.ws www.barman.ws/wisp

%C 201 W. 103rd Street, Indianapolis, IN 46290

%D 2002

%G 1-57870-264-X

%I Macmillan Computer Publishing (MCP)/New Riders

%O U\$34.99/C\$52.95/UK#27.50 800-858-7674 317-581-3743 info@mcp.com

%P 216 p.

%T "Writing Information Security Policies"

Until recently, the classic resource for those charged with writing security policies was "Information Security Policies Made Easy" (cf. BKISPME.RVW). Trouble was, that book made it a little bit too easy: the format encouraged people to use pieces without modification, and one size, in the security field, definitely does not fit all. This book, however, takes the opposite approach. While still aimed at the non-technical manager responsible for producing the policy, it uses minimal examples, concentrating on the process of policy formation.

Part one looks at starting the process. Chapter one defines what policies are and why they are important, and outlines the first steps needed to proceed. A good, broad outline of what your company should have in the way of a policy comes in chapter two. Finally, the responsibilities of different departments; their activities and roles; are presented in chapter three.

Part two covers the main body of security policy development. Chapter four starts out with physical security. As noted above, readers will have to go beyond the example policies given in the text, but these samples do provide a reasonable guide for what the final items should look like. Authentication and network security is dealt with in chapter five, although the telecommunications material is quite limited. Some of this lack is made up in chapter six's review of Internet policy, which goes beyond

firewalls

to examine training, applications, e-commerce, and other areas.

E-mail use

has a set of special requirements separate from those of the net, and these

are addressed in chapter seven. Unfortunately, as with all too many works,

the review of malware policies, in chapter eight, is weaker than the rest of

the book. (Does the example policy to use "all means to prevent the spread

of computer viruses" mean that you can't use Microsoft products? And why,

in this day and age of "fast burner" e-mail viruses, is a signature update

every thirty days deemed sufficient?) The limited technical background also

contributes to the frailty of chapter nine's overview of encryption. Some

policies are too broad, while there are missing areas that may need to be

addressed, depending upon industry and operations. Chapter ten has very

solid coverage of application development policies, which are all too often

neglected in other works.

Part three is concerned with maintaining the policies. Chapter eleven seems

slightly off topic, as it deals with acceptable use policies.

However,

chapter twelve looks at the roles and responsibilities involved in

compliance and enforcement. A short precis of the policy review process

ends the book in chapter thirteen.

While not a panacea, this book is clear, well written, and helpful. There

is valuable advice packed into few enough pages that a manager should be

able to read it on a cross-country plane trip.

copyright Robert M. Slade, 2002 BKWRINSP.RVW 20020601
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

<http://victoria.tc.ca/techrev> or <http://sun.soci.niu.edu/~rslade>



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 18

Saturday 27 July 2002

Contents

- [Gridlock as 800 London traffic lights seize](#)
[Adrian Lightly](#)
- [Nasdaq glitch hits stocks starting with 'M' or 'N'](#)
[Joan Lee Brewer](#)
- [Princeton admissions office caught breaking into Yale computers](#)
[Steve Klein](#)
- [Warchalking the Networks](#)
[Chris Leeson](#)
- [Handspring hands out names and springs out numbers](#)
[Monty Solomon](#)
- [Risks from cyberterrorism](#)
[NewsScan](#)
- [American style cyber warfare: what are the risks?](#)
[Hendrik](#)
- [No more JPEGs - ISO to withdraw image standard](#)
[Monty Solomon](#)
- [Reinventing read-only disks](#)
[Jeremy Epstein](#)
- [Possible day-of-week error - Zeller](#)
[John Stockton](#)

- [Finger-printing children in schools, without parental involvement](#)
[Peter Houppermans](#)
 - [Apple OSX and iDisk and Mail.app](#)
[Randal L. Schwartz](#)
 - [Re: Listen to TCAS, not the controller!](#)
[Bob Morrell](#)
 - [Re: E-mail content filtering ...](#)
[Anthony W. Youngman](#)
[Nick Brown](#)
[Marc Horowitz](#)
[Robert Woodhead](#)
 - [Re: Uselessness of "Dirty word" filters](#)
[J.D. Abolins](#)
[Danny Lawrence](#)
 - [news@sei interactive--Second quarter 2002 issue available](#)
[Hollen Barner](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Gridlock as 800 London traffic lights seize

Adrian Lightly <adrian@pigeonhold.com>

Thu, 25 Jul 2002 09:55:35 +0100

Central London was brought to a standstill in the rush hour today when 800 sets of traffic lights failed at the same time -- in effect locking signals on red.

[http://www.thisislondon.com/dynamic/news/top_story.html?
in_review_id=649242&in_review_text_id=620267](http://www.thisislondon.com/dynamic/news/top_story.html?in_review_id=649242&in_review_text_id=620267)

[http://www.thisislondon.com/dynamic/news/top_story.html
?in_review_id=649242&in_review_text_id=620267](http://www.thisislondon.com/dynamic/news/top_story.html?in_review_id=649242&in_review_text_id=620267)

Oops.

I liked this bit:

"The worst gridlock the capital has seen for years was caused by a computer which crashed as engineers installed software designed to give pedestrians longer to cross the roads."

So, in essence, that worked perfectly. Testing complete.

[Are you longing to cross the road on red? PGN]

⚡ Nasdaq glitch hits stocks starting with 'M' or 'N'

"Joan Lee Brewer -- CSE" <joanbrewer@attbi.com>
Wed, 24 Jul 2002 11:57:51 -0700

Six days before it is set to launch a new trading platform, the Nasdaq Stock Market experienced a glitch as its systems accidentally rebroadcast the day's data for stocks beginning with the letters 'M' and 'N'. That resulted in daily volumes figures appearing much higher than they actually were for the affected stocks [with Microsoft, Nextel, and Novellus being listed among the top 10 movers]. [PGN-ed from Reuters item, 23 Jul 2002]
<http://news.moneycentral.msn.com/ticker/article.asp?Feed=RTR&Date=20020723&ID=1802531&Symbol=US:MSFT>
<http://news.moneycentral.msn.com/ticker/article.asp?Feed=RTR&Date=20020723&ID=1802531&Symbol=US:MSFT>

⚡ Princeton admissions office caught breaking into Yale computers

Steve Klein <steveklein@mac.com>

Fri, 26 Jul 2002 15:51:26 -0400

The 26 Jul 2002 issue of the **Wall Street Journal** carried an article by Charles Forelle detailing how the Princeton admissions office was caught "accessing confidential Internet records to see whether its rival had admitted or rejected students who had applied to both schools." Princeton suspended, with pay, associate dean and director of admissions Stephen LeMenager, pending an investigation of the incident.

"Princeton was able to use the publicly available Yale.edu1 Web site to get the confidential admissions data because it had the students' passwords -- the names, Social Security numbers and dates of birth they had provided on their Princeton applications."

After hearing rumors about Princeton accessing their site, Yale officials reviewed access logs for the site and discovered that computers using IP addresses belonging to Princeton had accessed the site. Yale contacted the students to ask if they had used computers near Princeton to check their accounts. No one said yes. The IP addresses were traced to the Princeton admissions office.

"Lauren Weinstein, the founder of the Privacy Forum, an electronic-rights group, said Princeton's actions were clearly wrong, but Yale's site should not have relied on Social Security numbers and birth dates, which can

sometimes be retrieved from public records, to secure the data."

Excerpted and paraphrased from the Wall Street Journal article found here:

<<http://online.wsj.com/article/0,,SB1027628736531063280.djm,00.html>>

(subscription required)

Steve Klein 1-248-YOUR-MAC-EXPERT (248-968-7622)

✶ Warchalking the Networks

"LEESON, Chris" <CHRIS.LEESON@london.sema.slb.com>

Fri, 26 Jul 2002 09:47:00 +0100

The 26 Jul 2002 *Metro* notes the appearance of strange chalk patterns on the streets of London. These consist of two semicircles, a circle, or a circumscribed W, with some numbers added.

"Far from being the work of aliens, they have been created by something even more sinister - computer geeks."

The symbols are the creation of one Matt Jones (a "British Internet expert"), and denote places where wireless connections to the Internet can be accessed. From what I can make out from the article the two semi-circles indicate an unsecured network, the circle indicates a closed network and the circumscribed W indicates secured network. The recording of this information is called "Warchalking".

Businesses claim that this is a major risk to security. That may

be so - it
is certainly not a good advertisement for the Business in
question (the real
threat to security is the Business that has not taken care to
secure it's
wireless network).

OK, not a new risk (Wireless LANs go back at least as far as
[Risks 10.83](#)),
but a more visible incarnation of an existing one.

✶ Handspring hands out names and springs out numbers

Monty Solomon <monty@roscom.com>

Fri, 26 Jul 2002 16:49:27 -0400

Customers received two surprises from Handspring this week: an e-mail
announcing the delay of the Treo handheld Treo 90 and Treo 270
(because of
faulty screen parts), and customer names, e-mail addresses and
phone numbers
of other Treo customers. Handspring confirmed that its customer
service
department inadvertently attached a spreadsheet with customer
information to
an e-mail sent to about 250 people who placed Treo orders in
recent days.

[Source: Richard Shim, CNET News.com, 26 Jul 2002, retitled and
PGN-ed]

<http://news.com.com/2100-1040-946624.html>

✶ Risks from cyberterrorism

"NewsScan" <newsscan@newsscan.com>

Thu, 25 Jul 2002 08:56:19 -0700

Cybersecurity experts are busy lobbying Congress for protections from liability lawsuits but some analysts say the media may be overstating the risks from terrorist cyber attacks. Marc Maiffret of eEye Digital Security says, "Terrorists are only recently starting to realize the benefits of having people within their organizations that have real hacking skills," and University of South California professor of communications Douglas Thomas adds: "Cyber-terrorism is a lot more difficult than many people assume." Even so, security expert Stanley Jarocki warns that terrorists could do a lot of damage by cracking U.S. corporate systems: "Today, some say it would be easier for a terrorist to attack a dam by hacking into its command-and-control computer network than it would be to obtain and deliver the tons of explosives needed to blow it up. Even more frightening, such destruction can be launched remotely, either from the safety of the terrorist's living room, or their hideout cave." [AP/USA Today 24 Jul 2002;

NewsScan Daily, 25 July 2002]

http://www.usatoday.com/tech/news/computersecurity/2002-07-24-cybersecurity-protection_x.htm

http://www.usatoday.com/tech/news/computersecurity/2002-07-24-cybersecurity-protection_x.htm

⚡ American style cyber warfare: what are the risks?

Hendrik <hiz/vgq8@islandnet.com>

Sat, 27 Jul 2002 17:19:11 +0900

According to CNET News.com, US Reps. Howard Berman, D-Calif., and Howard Coble, R-N.C., are planning to introduce a bill "that would permit copyright holders to perform nearly unchecked electronic hacking if they have a 'reasonable basis' to believe that piracy is taking place."

<http://news.com.com/2104-1023-945923.html>

I had already gotten a feeling of indigestion after researching the "palladium" issue, and now words are failing me - so may I ask the experts in this forum to share some of their insights about the proposed cyber warfare legislation and associated risks?

✶ No more JPEGs - ISO to withdraw image standard

Monty Solomon <monty@roscom.com>

Tue, 23 Jul 2002 20:13:59 -0400

The ISO standards body will take the unprecedented step of withdrawing the JPEG image format as a formal standard if Forgent Networks, a small Texan company, continues to demand royalties on a seventeen-year old patent. According to Richard Clark, JPEG committee member and JPEG.org webmaster, Forgent's royalty grab -- coming after two decades of royalty-free use -- means that ISO is obliged to withdraw the specification. [Source: Andrew

Orlowski, *The Register*, 23 Jul 2002]

<http://theregister.co.uk/content/4/26339.html>

✶ Reinventing read-only disks

"Jeremy Epstein" <jepstein@webmethods.com>

Thu, 25 Jul 2002 16:00:34 -0400

In the days when disk drives were expensive and the size of washing machines, they usually had a "read only" physical switch. Flip the switch, and no matter what the software did, it couldn't write to the disk, because the write circuitry was disabled.

Fast forward twenty years, where Scarabs Corp just introduced a disk drive with two heads and two cables. One cable is connected to a head (or more likely, a set of heads) that can read the disk and the other cable to an administrative computer that can both read and write the disk. Even if a hacker is successful at breaking into a system, they can't deface the web site.

Too bad we don't have those old fashioned switches.... with the exception that you couldn't simultaneously have one machine updating and another in read-only mode, it's pretty much the same deal.

Of course, none of these solutions are any good for web sites that need to update information on the fly (e.g., to put an order into a database).

Details at

<http://computerworld.com/securitytopics/security/story/0,10801,72943,00.html>

✦ Possible day-of-week error - Zeller

John Stockton <spam@merlyn.demon.co.uk>

Wed, 24 Jul 2002 18:37:22 +0100

Algorithms for determining the day-of-week from year-month-day - whether or not truly Zeller's - can, for certain dates, compute a negative number mod 7, which does not yield the desired result. Zeller himself dealt with this.

Tests using "current" dates in the later 1900's would not have seen this problem.

A good test date is 2001-03-01 (1st March 2001); the algorithm can easily be run manually.

The problem has been seen, for example, in C code in an Internet draft.

Those whose systems do suitable run-time checking may already have discovered the problem.

John Stockton, Surrey, UK. <http://www.merlyn.demon.co.uk/programs/>

Dates: miscdate.htm moredate.htm js-dates.htm pas-time.htm critdate.htm etc.

🔥 Finger-printing children in schools, without parental involvement

Peter Houppermans <Peter.Houppermans@paconsulting.com>

Mon, 22 Jul 2002 16:37:58 +0100

[Note the return of an old favourite: "People who have nothing to hide - why would they worry?" PH]

Row over finger-printing in schools

Source:

http://news.bbc.co.uk/1/hi/english/education/newsid_2144000/2144188.stm

Tens of thousands of children are being finger-printed in school -- often without the consent of their parents, a human rights group has complained. Prints are taken for a library lending system which the makers say makes lending more efficient and less vulnerable to abuse. But the pressure group Privacy International says the practice is illegal and breaches the human right to privacy.

[Dangerous]

One of the makers of the technology, Micro Librarian Systems (MLS), say they have sold about 1,000 systems to schools in the UK and abroad. Simon Davies, of the campaign group Privacy International says the practice is "dangerous, illegal and unnecessary". He says the use of the technology

should be banned in schools.

"It dehumanizes our children and degrades their human rights," he said.

"Such a process has the effect of softening children up for such initiatives as ID cards and DNA testing. It's clearly a case of 'get them while they're young'. They are seen as a soft target for this technology".

[Encrypted]

The group says it has been contacted by parents who are angry that they have not been asked for to give their consent for the finger-printing. Manufacturers MLS say it would be very difficult for a third party to access the prints and make use of them. The company's technology director Stephen Phillips said: "The system does not store the actual fingerprint, but a map of it which takes in the print's key features. "The image is then compressed and encrypted, so it would take a lot of effort to use it.

"People who have nothing to hide - why would they worry?"

Mr Phillips said the company advised schools to consult or inform parents before they used the technology. He said only two parents had complained about the use of the technology to the company.

Privacy International says it expects there to be legal challenges to the use of the technology in schools.

[Also commented on by Gary Barnes. PGN]

🔥 Apple OSX and iDisk and Mail.app

<Randal L. Schwartz>

24 Jul 2002 09:10:59 -0700

(From Bugtraq, submitted to RISKS by Monty Solomon)

(<http://online.securityfocus.com/archive/1/284087>)

The password for an Apple iDisk is sent via HTTPS/WebDAV. However, if you configure OSX with an iDisk password, the same password is copied to the Mail.app configuration (which might not have been previously configured). Clicking on a "mailto" link fires up Mail.app, which then connects to mac.com which *does not* support any method of encrypted password transmission.

Net effect: your iDisk password is transmitted in the clear without your awareness, albeit as a mail password.

Problems:

- mac.com SMTP doesn't support encrypted passwords
- mac.com's mail password is *always* identical to iDisk password
- OSX's "do what I mean" friendliness saves passwords without knowledge

🔥 Re: Listen to TCAS, not the controller! ([RISKS-22.15](#))

"Bob Morrell" <bmorrell@wfubmc.edu>

Thu, 25 Jul 2002 09:05:20 -0400

RISKS has for many years now provided us with commentary and insight into

the problems that result from trusting computers too much. I think more comment is due on the collision of a cargo plane and a Russian airliner, which could have been prevented if the Russian Pilot had trusted the computerized collision avoidance system (TCAS) rather than the human air controller. Marty Solomon noted the event in [RISKS-22.15](#).

There are several reported aspects of this event that deserve some thought. Every non pilot (and several private aircraft pilots who do not use TCAS) that I have spoken to, without exception, say they would have trusted the human air controller rather than the computer, this despite the fact that the human was miles away, using a remote sensing device and managing other problems. The TCAS, on the other hand, was right on the scene, directly communicating with the other plane's TCAS. The Hollywood portrayal of 'infallible' machines, and perhaps daily experience with modern PC's clearly has downgraded the public trust in automated devices. Western pilots, it was reported (NPR I believe), are trained to trust the TCAS over the human controller, Russian aviators the reverse, so it appears that the pilot was following his training, rather than deciding on the spur of the moment who to believe. Russian trainers are no doubt rethinking this policy. It would be interesting to learn the historical source for this difference in training. As with almost all major aviation disasters, multiple mistakes led to this crash. The decision to ignore the TCAS was the last in a series, and if the reports on the Russian training are correct, was not,

technically speaking, a mistake on the pilot's part, however horrific the results. The RISK of blind, unthinking MISTrust of computers, we now see, can be as great as the risk of blind trust. An educated understanding of the computerized systems that we use is essential. Public perception is, in my opinion, too monolithic. TCAS is a highly tested system with a flawless record; it cannot be compared to the computer program that calculates my power bill.

Bob Morrell, Cancer Center, <http://home.triad.rr.com/bmorrell/>

✉ Re: E-mail content filtering ... (Miller, [RISKS-22.16](#))

"Anthony W. Youngman" <Anthony.Youngman@ECA-International.com>
Thu, 25 Jul 2002 13:09:10 +0100

As I understand it, the main purposes of the filters is to control the amount of unsolicited (usually commercial) bulk e-mail a.k.a. spam. I've seen reports that UBE is a significant contributor to network infrastructure costs, which accrue to the recipient, not the sender. The filters do seem to be having some positive (from the recipients point of view) impact on the spam problem.

Something else to watch out for is legality ...

Certainly in the UK I do not know of any ISP that filters incoming mail.

There may be some, but none of the big boys (BT, Demon,

Freeserve that I know of) do. To do so without the explicit knowledge of their customers would almost certainly lay them open to charges of censorship, of unlawfully tapping and tampering with communications, etc etc.

Many ISPs do filter outgoing mail though. I know Pipex scan everything going out via their servers, as does (I believe) Freeserve. Freeserve go even further, forcing all outgoing SMTP through their mail proxies, which have sophisticated anti-spam checks.

They can get away with scanning outgoing mail because of AUPs and customer contracts, but scanning incoming mail would be legally very dangerous.

Cheers,
Wol

✶ Re: E-mail content filtering ... (Miller, [RISKS-22.16](#))

BROWN Nick <Nick.BROWN@coe.int>

Thu, 25 Jul 2002 18:35:24 +0200

IMHO, the problem stems (as usual!) from bad management, and to a lesser degree, to incompetent sysadmins (hired by the same bad managers).

What typically happens is that a bunch of users (say, not-very-computer-literate bosses - think Dilbert's pointy-haired boss) receive spam which they deem offensive (say, females receiving invitations

to p*rn sites, or males insulted by the suggestion that they need V*agra or other below-the-waist "enhancements"), and demand that "something must be done". Now in a 33.6K modem environment, spam is a waste of download time, but on a corporate LAN when mails are brought to your desk in real time, it really isn't much effort to click "delete", and after a few dozen, one can recognise 99% of spam from the title... if one cares to make the effort (not always a hallmark of the "PHB").

So, the PHB storms off to the IS department with cries of "stop this cr*p from getting through". Now, either the IS people are clued up - in which case they might or might not try to dissuade the PHB, depending on whether their previous experiences in the corporate culture lead them to believe that this is likely to be fruitful - or, in many cases, they aren't. Either way, it's likely that they will implement e-mail filtering with "a product", usually "the market leader", which in turn got to be that way by making the biggest and most far-fetched claims, while spending the minimum on R&D to actually get that way. Many of us have already been down exactly the same road with Web content filtering.

Most RISKS readers will, of course, be horrified by the idea that a spam filter could unintentionally block even a tiny percentage of non-spam mail. But I suspect that for the average PHB, not getting quite as many [genuine] e-mails as s/he currently does, might not be a bad thing. Less time spent typing (ugh!) and working out how blind copy works, etc. If

they do get
shouted at for not answering an important mail, well, they can
blame IS !

✶ Re: E-mail content filtering ... (Bourguignon, [R-22.17](#))

Marc Horowitz <marc@mit.edu>

24 Jul 2002 19:13:34 -0400

> * Just PGP signing an e-mail is enough to ensure that the e-
mail content is
> not altered without notice.

This is true. However, if it is altered, recovering the content
of
the original message may be difficult if you don't know what the
filter did. One can argue this is a feature, as the recipient
cannot
misunderstand what he cannot decode or decrypt.

>> * Just PGP encrypting is enough to ensure that the e-mail
content
>> cannot be filtered.

This is not true, and ignores the point of Bill Gunshannon's
original
post. It is nearly guaranteed that PGP's base64 encoding will
contain
words which may cause the e-mail to be modified or dropped.
Your dirty
jokes may get through, but your lunch plans with your mother may
not.
Of course, the presence of such words in the encoded ciphertext
is
completely uncorrelated to the presence of such words in the
plaintext, but explaining this to your PHB is up to you.

✉ Re: E-mail content filtering ... (Miller, [RISKS-22.16](#))

Robert Woodhead <trebor@animeigo.com>

Thu, 25 Jul 2002 19:56:56 -0400

>* Just PGP encrypting is enough to ensure that the e-mail content cannot be
> filtered.

Unfortunately, one of the most common and useful anti-spam heuristics is "e-mail contains none of the most common english words". This catches a lot of non-English spam and pure-html crud.

As the maintainer of a database of anti-spam heuristics (and previously, an anti-virus program author), the fact is that perfect spam detection is impossible, it's yet another variant of the halting problem.

I personally find that the most effective approach is spam-labelling; in other words, adding headers to suspect e-mail saying "I think this is spam, and this is why". Then let the user's e-mail app apply filtering rules using the additional context.

For example, I filter all e-mail marked as spam to the bottom of my inbox (lowest priority), then use other filtering rules to whitelist e-mail from known sources. I get over 300 spams a day but it takes only a few seconds to quickly scan them for false positives.

Robert Woodhead, Webslave & Mad Overlord <http://selfpromotion.com/>

⚡ Re: Uselessness of "Dirty word" filters (Lawrence, [RISKS-22.16](#))

"J.D. Abolins" <jda-ir@njcc.com>

Thu, 25 Jul 2002 08:16:41 +0000

Re: rejecting a horse named "Dr. Fager", I started to see other possible rejection problems.

Proper names: Would the name of the current USA President being interpreted as a vulgar term deserving filtering?

The possible derogatory term rejected by the DW filter Danny Lawrence encountered is also a British reference for a cigarette. (I guess some proponents of DW filters would consider cigarettes and smoking worth filtering out. But then how can one do an anti-smoking... oops,,, anti-[filtered]... education on the Web?)

Speaking of British terms, a recipes for some traditional British food dishes would run afoul of the filters:
"[filtered]ers and Mash"
"Spotted [filtered]"
"[filtered] in Gravy"

But "Bubble and Squeak" should be be safe. <g>

[Not entirely. PGN]

⚡ Re: Dirty word filters and Horse's names

"Danny Lawrence" <Danny@TiassaTech.com>

Thu, 25 Jul 2002 11:44:06 -0400

Actually horse's names are still limited to 18 letters and all names must be submitted to the Jockey Club for approval. There is an overview of allowable names here: <http://home.jockeyclub.com/rules/rules.html#rule6> (see, there is a "Rule 6"!). Also note the last rule "B. In addition to the provisions of this Rule, the Registrar of The Jockey Club reserves the right of approval on all name claiming requests." One owner, after having several names rejected by Buddy Bishop, the registrar, decided to call his horse "Buddy Named Me".

news@sei interactive--Second quarter 2002 issue available

Hollen Barmer <hlb@sei.cmu.edu>

Wed, 24 Jul 2002 11:18:15 -0400

The second quarter 2002 issue of news@sei interactive is now available.

The articles in this issue are

"Preventing Security-Related Defects"

"TIDE: Promoting Technology Adoption Through Technology Collaboration"

"First International Conference on COTS-Based Software Systems a Success"

"CERT/CC and Secret Service Collaborate on Security"

Our columns in this issue are

Watts New: "Surviving Failure"

The Architect: "Aligning Business Models, Business Architectures, and IT Architectures"

The COTS Spot: "Risk/Misfit Redux"

Security Matters: "Is There an Intruder in My Computer?"

news@sei interactive (<http://interactive.sei.cmu.edu/>) is a Web-based publication of the Software Engineering Institute (SEI). The news@sei interactive team is interested in your comments, questions, and suggestions for improvement. Contact us at interactive@sei.cmu.edu.

CERT, Capability Maturity Model, and CMM are registered in the U.S. Patent and Trademark Office. CMM Integration, CMMI, Personal Software Process, and Team Software Process are service marks of Carnegie Mellon University.



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 19

Monday 19 August 2002

Contents

- [Name filtering affects police officer](#)
[Fuzzy Gorilla](#)
 - [Massive ATM fraud after security problems due to Sept 11](#)
[Tom Van Vleck](#)
 - [A universal Turin machine?](#)
[PGN](#)
 - [Win32 API utterly and irredeemably broken](#)
[Monty Solomon](#)
 - [Microsoft EULA asks for root rights -- again](#)
[Monty Solomon](#)
 - [FTC Stamps Microsoft's Passport](#)
[Monty Solomon](#)
 - [Keystone SpamKops](#)
[Edward W. Felten](#)
 - [Re: Listen to TCAS, not the controller](#)
[Peter B. Ladkin](#)
 - [An automation-related AIRPROX incident](#)
[Peter B. Ladkin](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ Name filtering affects police officer

"Fuzzy Gorilla" <fuzzygorilla@euroseek.com>

Thu, 15 Aug 2002 18:41:31 -0400

It is not clear that we will ever solve the problem of computerized filtering based on "lewd" names when even humans can't get it right.

The badge of El Paso police officer Christine Lynn O'Kane (and her e-mail address) identified her as C. O'KANE (which unfortunately looks like 'cocaine'). After leaving the force for personal reasons and later reapplying, she was denied reinstatement on the grounds that her name was inappropriate -- despite her good service record that included an explicit recommendation her work file supporting her reinstatement. Although her appeal to the Civil Service Commission resulted in her being rehired, she has now reverted to her maiden name (Whitaker).

[Source: Cop In Trouble Over Name, AP, 12 Aug 2002; PGN-ed]

http://dailynews.yahoo.com/news?u=/ap/20020812/ap_on_fe_st/c_o_kane_1

✶ Massive ATM fraud after security problems due to Sept 11

Tom Van Vleck <thvv@multicians.org>

Mon, 5 Aug 2002 20:18:08 -0400

<http://fr.news.yahoo.com/020805/5/2pe9c.html>

[This is in French, but not yet reported in English.
Translation with the help of Babelfish. thvv]

4000 people are suspected of taking a total of \$15 million in ATM overdrafts from the NY Municipal Credit Union, whose computer system was damaged by 9/11 attacks and the phone and electric outages that followed. The CU chose to allow withdrawals of up to \$500/day without checking. Word got around. One person withdrew over \$18,000 in 54 transactions.

✶ A universal Turin machine?

"Peter G. Neumann" <neumann@csl.sri.com>
Mon, 19 Aug 2002 15:06:53 PDT

Seeing the number 4000 in the foregoing message from Tom Van Vleck reminded me of an article I read 12 days ago in *The Herald Tribune* Italian edition supplemental highlights from *Corriere della Sera* in English, 7 Aug 2002:
Police probe credit card scam. Turin police obtained a cigarette-pack-sized machine that been used by an up-scale restaurant to make about 4000 perfect-copy credit cards from cards used by customers, including mag stripes. The Clone Arranger Strikes Again. (The Shrewd of Turin?)

✶ Win32 API utterly and irredeemably broken

"monty solomon" <monty@roscom.com>

Mon, 19 Aug 2002 12:44:53 -0400

Thomas C Greene in Washington, 7 Aug 2002

Windows might possibly be the most insecure piece of viral code ever to infect a computer, according to Chris Paget who's found a fascinating hole in the Win32 Messaging System which he believes is irreparable, and which he posted to the BugTraq security mailing list.

The research leading to this discovery was inspired by MS Veep Jim Allchin, who testified to the effect that if flaws in the Windows Messaging System were sufficiently understood, national security would be deeply compromised, CRUISE missiles would be launched remotely, and /bin/laden would most likely find some novel way of raping your daughter with his big bad mou Paget has brought at least some of Allchin's fears to fruition ...

<http://www.theregus.com/content/55/25883.html>

Microsoft EULA asks for root rights -- again

Monty Solomon <monty@roscom.com>

Sun, 4 Aug 2002 23:03:51 -0400

Andrew Orlowski in **The Register**, London, 2 Aug 2002

An addition to Microsoft's End User Licensing Agreement has alarmed **Register** readers. Windows XP Service Pack 1 and Windows 2000

Service Pack

3 contain a new condition which asks you to allow Windows to go and install future updates. "You acknowledge and agree that Microsoft may automatically check the version of the OS Product and/or its components that you are utilizing and may provide upgrades or fixes to the OS Product that will be automatically downloaded to your computer," is the new bit you'll be interested in. ... <http://www.theregister.co.uk/content/4/26517.html>

⚡ FTC Stamps Microsoft's Passport

Monty Solomon <monty@roscom.com>

Fri, 9 Aug 2002 18:05:42 -0400

FTC Stamps Microsoft's Passport

Yesterday Microsoft settled a complaint by the Federal Trade Commission that its Passport user-ID service had violated its own privacy policy and was insufficiently secure. Almost every outlet featured the story prominently, and the Wall Street Journal e-mailed one of its infrequent Technology Alerts yesterday after the FTC/Microsoft conference call. ... <http://newsletter.mediaunspun.com/index000018770.cfm#a86817>

⚡ Keystone SpamKops

"Edward W. Felten" <felten@CS.Princeton.EDU>

Fri, 16 Aug 2002 09:45:06 -0400

I recently set up a web site at www.freedom-to-tinker.com. It's a weblog containing my commentary on various issues. Earlier this week, my ISP shut off the site, because the site had appeared on a list of "spammers" published by an outfit called SpamCop.

Apparently, this happened because one person, whose identity I was not allowed to learn, had sent SpamCop an accusation saying that he had received an unwanted e-mail message, which I was not allowed to see, that did not come from me but that did mention my web site. On that "evidence" SpamCop declared me guilty of spamming and decreed that my site should be shut down. Never mind that I had never sent a single e-mail message from the site. Never mind that my site was not selling anything.

Naturally, I was not allowed to see the accusation, or to learn who had submitted it, or to rebut it, or even to communicate with an actual human being at SpamCop. You see, they're not interested in listening to complaints from spammers.

With help from my ISP, I eventually learned that the offending message was sent on a legitimate mailing list, and that the person who had complained was indeed subscribed to that list, and had erroneously reported the message as unsolicited. Ironically, the offending message was sent by someone who liked my site and wanted to recommend it to others. Everybody involved (me,

my ISP, the person who filed the complaint, and the author of the message) agreed that the report was an error, and we all told this to SpamCop. Naturally, SpamCop failed to respond and continued to block the site.

Why did my ISP shut me down? According to the ISP, SpamCop's policy is to put all of the ISP's accounts on the block list if the ISP does not shut down the accused party's site.

Note the similarities to the worst type of Stalinist "justice" system: conviction is based on a single anonymous complaint; conviction is based not on anything the accused did but on favorable comments about him by the "wrong" people; the evidence is withheld from the accused; there is no procedure for challenging erroneous or malicious accusations; and others are punished based on mere proximity to the accused (leading to shunning of the accused, even if he is clearly innocent).

Note also that the "evidence" against me consisted only of a single unsigned e-mail message which would have been trivial for anyone to forge. Thus SpamCop provides an easy denial of service attack against a web site.

The only bright spot in this picture is that our real justice system allows lawsuits to be filed against guys like SpamCop for libel and/or defamation. My guess is that eventually somebody will do that and put SpamCop out of business.

[By the way, there is more discussion of this incident on my

blog site at

<http://www.freedom-to-tinker.com>

EWf]

✦ **Re: Listen to TCAS, not the controller (Morell, [Risks 22.18](#))**

"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>

Thu, 15 Aug 2002 11:38:00 +0200

In [RISKS-22.13](#), Bob Morell discusses the midair collision on 1 Jul 2002 over Southern Germany, in which a Bakshirian Airlines Tupolov 154, operating as BTC 2937, collided with a DHL Boeing 757-200, operating as DHX 611, although both were using ACAS II-compliant collision-avoidance systems, namely Honeywell TCAS II Version 7 systems [1] (TCAS is "kit"; ACAS II is the international designation for a requirement which TCAS II Version 7 fulfills).

Morell is right in saying that more comment is due on this accident.

However, his comment is misleading, particularly because of its superficial plausibility. Most misleading of all is the title suggestion that the crew of BTC 2397 (BTC CRW) should have listened to TCAS rather than the controller. To the contrary, their cognitive model may well have been such that prioritising the controller's advisory over the Resolution Advisory (RA) from TCAS would have been the most rational decision to make, as I note below.

An extended version of my comment is available as "ACAS and the South German Midair", RVS-Occ-02-02, on <http://www.rvs.uni-bielefeld.de>

First, a brief explanation of how TCAS II avionics operates [2,3]. TCAS II broadcasts signals on the radar-interrogation frequency, and receives responses from other aircraft's transponders. A Mode C transponder is a device which responds to radar beams of a certain frequency with information on the aircraft's identity and its "pressure altitude" - the altitude at which it would be flying in an "international standard atmosphere" at the measured outside air pressure. Additionally, the Mode S transponder used with TCAS II may receive and transmit messages, a facility used essentially in TCAS II.

TCAS II gives two types of advisories, Traffic Advisories (TAs) and Resolution Advisories (RAs). It displays the approximate relative position and separation of conflicting traffic visually on a display screen, and announces the advisory via simulated voice. TAs alert a crew to the presence of a potentially conflicting aircraft (determined by presence within a specified volume of surrounding airspace), and attempts to predict time-to-go to collision (TTG). When TTG reaches a certain threshold, a TA is generated; when TTG reaches a lower threshold, an RA is generated upon negotiation with the other aircraft's TCAS II, if it is so equipped. A TA is just a warning; pilots are not expected to manoeuvre in response to a TA. An

RA is an advisory to climb, or to descend. An algorithmic negotiation between the TCAS II avionics on both aircraft ensures that one aircraft of a TCAS-II-equipped conflicting pair receives a climb RA and the other a descend RA.

Morell speculates whether BTC CRW made a "mistake" or not, and suggests that the descent decision and action "if the reports on the Russian training are correct, was not, technically speaking, a mistake on the pilot's part...."

It is not clear to me what Morell's concept of a "mistake" is. First, any pro forma operational suitability of BTC CRW's actions is determined by German aviation law and associated approved procedures in German airspace, not by any "Russian training". Second, in private correspondence, Morell suggested that the RTC CRW action was "obviously" a mistake, since the two aircraft collided. I don't know what it would mean for the action to be a mistake, but at the same time not to be "technically speaking" a mistake. Besides, the criterion offered is clearly insufficient: DHX CRW action led just as inexorably to the collision, but it would be anachronistic to refer to this action as a "mistake".

I feel such speculation about possible pilot error without a careful analysis of the interactions in the cockpits, as contained on the cockpit voice recorder (CVR), is unwarranted. The CVR often provides the only means of assessing the quality of CRW decision making, and in this menage a trois

equipages in which four of the five participants are dead, I think such analysis is essential.

Morell says, astoundingly, that "TCAS is a highly tested system with a flawless record", apparently not counting this midair as a failure. On the contrary, the TCAS avionics were a causal factor in this accident: had neither aircraft been so equipped, the accident would not have happened (DHX CRW would have maintained altitude as cleared; BTC CRW would have descended as cleared and as they did; the aircraft would have missed each other by 600ft).

The TCAS system, like most complex systems which depend essentially on human action, does not have a "flawless record", even previous to this accident. There are significant operational issues with previous TCAS versions (such as 6.02 and 6.04a), which remain (while reduced) with TCAS II Version 7. Eurocontrol training materials say that TCAS "... cannot eliminate all risks of collision. Additionally, as in any predictive system, it might itself induce a risk of collision" [4, p17]. The Eurocontrol ACAS Operational Evaluation indicates a substantial history of false positives ("unnecessary RAs") [5]; the latest version, Version 7, shows a "40% reduction in unnecessary RAs" [6].

False positive RAs are not merely a nuisance; in dense traffic areas, which is where RAs are most likely to be generated, manoeuvres in accordance with RAs disrupt ATC planning and generate immediately an unanticipated higher

workload for a controller, which can be a safety risk when a controller is operating near the limits of higher capacities. There has been a significant rate of "nuisance" advisories, and one can anticipate pilots' reactions to the system crying "wolf" too often. Lincoln Labs apparently reported that that over 50% of RAs occurring in U.S: airspace are ignored [5, Section 5.3, p19].

Such operational issues arise with, for example, "stacks" of aircraft queuing for approach to an airport in instrument meteorological conditions, and in the European Reduced Vertical Separation Minimum airspace, introduced this year between Flight Levels 290 and 410 (between 29,000 ft and 41,000 ft in an "international standard atmosphere"). In both of these cases, aircraft are operating as cleared with only one thousand feet of nominal vertical separation. Altitude measuring equipment is allowed to be up to +/- 64 ft deviant in RVSM airspace, and altitude reporting equipment reports in either 25ft or 100ft increments. Two TCAS-equipped aircraft operating as cleared may well "see" each other separated by less than 850 ft, sufficient to generate a "nuisance" TA. Add effects of turbulence, or of a non-perfectly executed levelling off manoeuvre at a new cleared altitude ("bump up" or "bump down") and a "nuisance" RA can easily be generated [7].

One should not identify an ACAS II-compliant system with the TCAS II Version 7 avionics alone. The avionics influence an aircraft's flight path only through the crew's decisions and actions. The procedures which

crew are advised to follow, and their understanding of the situation (their "cognitive model") are essential components of the ACAS system. Not only that, but it is possible for misleading controller advisories to alter the cognitive model of one or more of the crew involved, indicating that the controller's role must be considered in any safety analysis of ACAS operation.

Facts already available concerning the July 1 midair collision highlight certain difficulties with ACAS operation, namely that ACAS does not handle some three-aircraft conflicts well. Consider the situation engendered by the circumstances on July 1.

We may assume that BTC CRW and DHX CRW knew that there were only two ACAS-equipped aircraft involved in the conflict. This information would be displayed; BTC CRW would see DHX at their 10 o'clock position (60 degrees left of straight ahead). However, at 23:25:03, 7 seconds after the first RA, BTC CRW were informed by air traffic control that there was conflicting traffic at their 2 o'clock position (60 degrees right of straight ahead) [1]. This aircraft was not on their display - indeed was not there; the controller's advisory was a cognitive mistake. BTC CRW is now faced with the following situation: there is a conflict with traffic painted by TCAS at their 10 o'clock position and also with non-painted traffic at their 2 o'clock position. Their cognitive model poses a three-aircraft conflict

situation. (One of these aircraft is a "ghost" but they do not know it.)

The importance of this scenario does not depend on what did or did not happen in the accident on July 1. We may find out from CVR and other evidence, or we may not, what BTC CRW's cognitive model actually was. The importance lies in that it is an ACAS scenario whose components have actually occurred, and therefore it must be analysed as part of a safety assessment of ACAS.

Let me use "Aircraft A" for the DHX-similar aircraft, "Aircraft B" for the BTC-similar aircraft, and "Aircraft C" for the aircraft at Aircraft B's 2 o'clock position. Since TCAS is not painting Aircraft C, Aircraft B CRW can suppose that Aircraft C will not be involved in any RAs. It is hard to say what cognitive model Aircraft A CRW have, since they might not have heard or assimilated the controller's mistaken advisory to Aircraft B CRW. So I shall not consider their cognitive model. Aircraft B CRW do not know whether the controller is in contact with Aircraft C or not, although it might be reasonable to suppose so. ATC has issued a descent instruction to Aircraft B to take Aircraft B out of conflict with Aircraft C. Further, Aircraft B have received an RA to climb. They can conclude that the RA was negotiated with Aircraft A, since their TCAS display is painting Aircraft A as the "intruder", and that Aircraft A has received a descent RA.

There is a clear strategy for Aircraft B CRW to follow when both controller's advisory and RA agree. They follow it. They then

come to be in further trouble only if Aircraft A manoeuvres in the reverse sense to their presumed RA. However, a dilemma is directly posed if the controller's advisory and the RA do not agree in sense. One rational strategy could be termed "better the devil you know". Aircraft B CRW can follow the controller's advisory to avoid Aircraft C, and attempt to use the TCAS display information to acquire Aircraft A visually and avoid it. They could also attempt to reduce speed to give greater TTG until conflict with Aircraft A.

Risky as this is, I see no more rational strategy available to Aircraft B CRW. Not even this meagre strategy is available if they are in Instrument Meteorological Conditions.

The manoeuvres of BTC CRW on July 1 are consistent with this strategy, which violates the oft-repeated advice to pilots not to manoeuvre contrary to an RA. I suggest on the basis of this scenario that this advice is not universally applicable. Indeed, the benefit of ACAS in this situation to Aircraft B is in knowing roughly where Aircraft A is - a benefit provided equally well by TCAS I, which does not generate RAs at all.

I believe this scenario shows that it is illusory to imagine that better or more uniform training will resolve ACAS operability problems. Before solutions can be trained, we first need a solution, and I doubt there is one for this scenario based on ACAS technology. I refer to my extended note for

other cases, involving three ACAS-II equipped aircraft, for which it is also unclear to me that a solution exists.

Peter B. Ladkin, University of Bielefeld, <http://www.rvs.uni-bielefeld.de>

References

[1] Bundesstelle fuer Flugunfalluntersuchung, Presseinformation, Zusammenstoß am Bodensee (available also in English), reviewed July 28th, 2002, <http://www.bfu-web.de/aktuinfo-d28.htm>

[2] Mitre Corporation, Center for Advanced Aviation System Development (CAASD), Traffic Alert and Collision Avoidance System, <http://www.caasd.org/proj/tcas/>

[3] Honeywell, Inc. Advanced Collision Avoidance Systems, at <http://www.honeywelltcas.com>

[4] Eurocontrol, ACAS II Training Manual, Version 2, available from <http://www.eurocontrol.int> -> Projects -> ACAS -> Training Materials
-> Training Manual Version 2, May 2000.

[5] Eurocontrol Experimental Center, European ACAS Operational Evaluation, Final Report, Eurocontrol Experimental Center Report No. 316, July 1997, available at <http://www.eurocontrol.fr> -> Documents -> (Search) Final Report 316
-> Reports for the Year 1997 -> 316.

[6] Mitre Corporation, Center for Advanced Aviation System Development (CAASD), Traffic Alert and Collision Avoidance System, <http://www.caasd.org/proj/tcas/>

[7] Eurocontrol, ACAS II Operations in the European RVSM Environment,

Project ACTOR, available from
<http://www.eurocontrol.int> -> Projects -> ACAS -> Training
Materials
-> Brochure f11, 2 August 2001.

✶ An automation-related AIRPROX incident

"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>

Thu, 15 Aug 2002 16:07:31 +0200

On 2 Oct 2000, there was a loss of separation (an AIRPROX incident in jargon) on the North Atlantic Track E from Europe to North America between an Airbus A330 and an Airbus A340 aircraft. The aircraft were operating under Reduced Vertical Separation Minima (RVSM), in which high-altitude aircraft may use a nominal vertical separation of 1,000 ft from each other for their operations instead of 2,000 ft, which has been standard. RVSM had been introduced for trials on the North Atlantic track system, and was introduced in European airspace in January 2002. RVSM depends essentially on participating aircraft using Airborne Collision Avoidance System (ACAS) equipment. Both incident aircraft were using Traffic alert and Collision Avoidance System (TCAS) Version 6.04 avionics.

I shall describe the incident briefly, omitting some salient observations made in the report. Since the report is about eleven A4 pages of prose and data, I recommend reading it in full [1].

The A340 was cleared at Flight Level (FL) 360 (the altitude at which the air pressure is the same as that at 36,000 ft in an International Standard Atmosphere), and the A330 at FL 370. The A330 was roughly abeam and slowly overtaking the A340, when the aircraft encountered clear air turbulence, described by the A340 captain as severe.

The A340 entered a "zoom climb", and went up to FL384, some 2,400 ft above its assigned FL and 1,400 ft above the FL assigned to the A330. Both aircraft had been receiving Traffic Advisories (TAs) on each other for some minutes before the incident, and during the incident received TCAS Resolution Advisories (RAs); the A340 was advised to descend and the A330 to climb. The A330 captain said that the A340 passed through his FL, some 200-300ft to his left, before he had time to react to the RA. The maximum rate of climb of the A340 during the incident was recorded to be some 6,000 ft/min.

At the time the first RAs were issued, the aircraft were likely separated by some 800 ft, and the RAs were "nuisance" RAs due to the turbulence, as described in [2]. The A340 had not begun its zoom climb. About ten seconds later, though, the A340s flight control system captured "alpha prot", and the A340 commenced its climb. "Alpha prot" is a value of a flight parameter known as the "phase-advanced angle of attack" which triggered a change from the "normal" flight control law in the Airbus fly-by-wire control system to the "angle of attack protection" law, or AoA law. When both

control

sidesticks remain neutral, AoA law attempts to maintain the angle of attack (inclination of the aircraft's wing to the air it is flying through; the major parameter used in controlling lift in flight) at the value it has at the point of reversion. One may presume that the turbulence encountered had momentarily increased the angle of attack to a high value at the time that alpha prot was captured.

Right before alpha prot was captured, the A340's airspeed briefly rose above its "limiting value" of 0.86 Mach (0.86 times the speed of sound at that altitude), due to the turbulence encounter. This triggered a Master Warning, and also disconnected the autopilot. The Fault Warning Computer prioritises warnings, and the autopilot disconnect warning was suppressed for about six seconds in favor of the Master Warning. It is surmised that the crew may not have registered the TCAS RA because of the interference of the other warnings. The crew responded right away (within five seconds) to the Master Warning by reducing thrust.

The investigation suggests that, because of the fluctuations caused by the turbulence, the reversion from normal law to AoA law would likely not have been sensorily detected. Furthermore, this reversion is not possible under autopilot control. It is likely that the crew then had, for up to six seconds, no obvious reason to judge that the aircraft was operating in AoA law.

The investigators say that "Such was the vigor of the A340's climb in AoA law, the aircraft could well have climbed through FL 363 (thus provoking a TCAS RA with revised software version 7.0) in a very short time, even if the crew had applied nose-down sidestick as soon as they heard the (delayed) autopilot disconnect warning. The climb to FL 363 would have been sufficient to generate a TCAS RA in any adjacent aircraft at FL 370 but, if the intruder aircraft continues its climb, there can be no guarantee that an aircraft directly above it could respond in sufficient time to avoid a collision."

The incident raises the issue of operations under RVSM. The investigators recommended suggested that such an incident is relevant to the safety case being made at that time for the introduction of RVSM in Europe. The incident shows that that a combination of a turbulence encounter, automated flight control, and RVSM could prove deadly, with or without improved versions of TCAS.

Peter B. Ladkin, University of Bielefeld, <http://www.rvs.uni-bielefeld.de>

References

[1] U.K. Air Accidents Investigation Branch, AAIB Bulletin 6/2001, Ref. EW/C2000/10/2, <A HREF="<http://www.aaib.dft.gov.uk/bulletin/jun01/cggwd.htm>"><http://www.aaib.dft.gov.uk/bulletin/jun01/cggwd.htm>

[2] Eurocontrol, ACAS II Operations in the European RVSM Environment,

Project ACTOR, available from

<A HREF="<http://www.eurocontrol.int>"><http://www.eurocontrol.int> ->

Projects -> ACAS -> Training Materials

-> Brochure f11, 2 August 2001.



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

[ACM](#) Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 20

Thursday 22 August 2002

Contents

- ["Homeland Insecurity"](#)
[Monty Solomon](#)
- [Home overvalued by \\$200 million affects tax recovery](#)
[Fuzzy Gorilla](#)
- [103-year-old man told to bring parents for eye test](#)
[Arthur Goldstein](#)
- [Alleged ID thief arrested in NYC](#)
[Monty Solomon](#)
- [Your packets know the way to San Jose.](#)
[Malcolm Purvis](#)
- [Emergency call-center power-supply woes](#)
[Dave Stringer-Calvert](#)
- [YASST: Yet Another Silly Spam Trick](#)
[Rob Slade](#)
- [Re: E-mail content filtering ...](#)
[Joe Stoy](#)
- [E-mail *envelope* filters blocking NDN and DSN](#)
[MATteo HCE Valsasna](#)
- [Content based e-mail filtering -- timely example](#)
[Betsy Schwartz](#)

- [Klez + html login = no security](#)
[Leonard Erickson](#)
 - [Klez: The Virus That Won't Die](#)
[Monty Solomon](#)
 - [The left hand of the government asketh ...](#)
[Rob Slade](#)
 - [Re: Apple OSX and iDisk and Mail.app](#)
[Dave](#)
 - [REVIEW: "Computers and Ethics in the Cyberage", Hester/Ford](#)
[Rob Slade](#)
 - [SAFECOMP 2002 & ECCE-11](#)
[Massimo Felici](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ "Homeland Insecurity"

Monty Solomon <monty@roscom.com>

Wed, 14 Aug 2002 10:16:15 -0400

Charles C. Mann, a top expert, says America's approach to protecting itself will only make matters worse. Forget "foolproof" technology -- we need systems designed to fail smartly...

To stop the rampant theft of expensive cars, manufacturers in the 1990s

began to make ignitions very difficult to hot-wire. This reduced the

likelihood that cars would be stolen from parking lots-but apparently

contributed to the sudden appearance of a new and more dangerous crime, carjacking.

After a vote against management Vivendi Universal announced earlier this

year that its electronic shareholder-voting system, which it had adopted to tabulate votes efficiently and securely, had been broken into by hackers. Because the new system eliminated the old paper ballots, recounting the votes-or even independently verifying that the attack had occurred-was impossible.

To help merchants verify and protect the identity of their customers, marketing firms and financial institutions have created large computerized databases of personal information: Social Security numbers, credit-card numbers, telephone numbers, home addresses, and the like. With these databases being increasingly interconnected by means of the Internet, they have become irresistible targets for criminals. From 1995 to 2000 the incidence of identity theft tripled.

<http://www.theatlantic.com/issues/2002/09/mann.htm>

[This article is extremely timely, well written, and important for RISKS readers. It also features various insights from Bruce Schneier, whom Charles interviewed while researching the article. PGN]

🔥 Home overvalued by \$200 million affects tax recovery

"Fuzzy Gorilla" <fuzzygorilla@euroseek.com>

Mon, 19 Aug 2002 16:20:50 -0700

In Manhattan, Kansas, a home property valued at \$59,500 was

inadvertently
changed to \$200,059,000, and seriously disrupted the calculation
of the
local budgets for the school district, the city, and Riley
County --
resulting in a 6.5% overstatement of the value of county
property, and a
shortfall in tax revenues of over \$2.3 million. [PGN-ed]
[http://dailynews.yahoo.com/news?u=/ap/20020819/ap_on_fe_st/
property_value_2](http://dailynews.yahoo.com/news?u=/ap/20020819/ap_on_fe_st/property_value_2)

✶ 103-year-old man told to bring parents for eye test

<arthur.goldstein@att.net>
Fri, 02 Aug 2002 01:14:55 +0000

Another cute medical mix-up (Reuters, 31 Jul 2002):
[http://news.excite.com/odd/article/
id/256255|oddlyenough|07-31-2002::12:22|reuters.html](http://news.excite.com/odd/article/id/256255|oddlyenough|07-31-2002::12:22|reuters.html)

British pensioner Joseph Dickinson, 103, had a shock when his
local hospital
called him in for an eye test and told him to bring his
parents. "I must be
getting younger, in fact much younger," he told his local paper,
the
Hartlepool Mail. He was born in 1899, but because the hospital
computer
only read the last two digits it mistook his age as just three
years old. ...

✶ Alleged ID thief arrested in NYC

Monty Solomon <monty@roscom.com>
Tue, 20 Aug 2002 22:17:56 -0400

A man captured by the US Marshals Service in New York is accused of stealing the identities of 12 Boston lawyers to buy lavish cars and finance spending sprees, the agency said yesterday. Shawn R. Pelley, 26, had evaded authorities for nearly a year before he was caught after a car chase. Once convicted of fraud, he allegedly began an identity-theft scam shortly after his release from prison last summer. Using information from a law directory, he allegedly obtained his victims' birth certificates and credit reports, opened credit-card accounts, and took bank loans on the stolen IDs.

[Source: Thanassis Cambanis, *The Boston Globe*, 20 Aug 2002; PGN-ed]

<[http://www.boston.com/dailyglobe2/232/metro/Alleged ID thief arrested in NYC+.shtml](http://www.boston.com/dailyglobe2/232/metro/Alleged_ID_thief_arrested_in_NYC+.shtml)>

✶ Your packets know the way to San Jose.

Malcolm Purvis <malcolmpurvis@optushome.com.au>

Wed, 21 Aug 2002 22:32:00 +1000

The Southern Cross Cable Network, a significant supplier of bandwidth between Australia and the US, recently announced a new access point in San Jose. The Associated Press release says in part:

The new San Jose access point is located at Market Post Tower, which currently houses the world's most famous Internet peering point, MAE

West. Virtually all of the network access points and data centers in the surrounding San Francisco Bay Area connect to Market Post Tower via high-speed local fiber rings. ... 70% of the Internet traffic from the Western United States and 40% of the world Internet traffic passes through the building that houses the new Southern Cross access point.

I wonder how well the rest of the Internet would cope if something happened to that building (which has a web site, so you can learn all about it). I also see that MAE West is owned by WorldCom.

The press release is at:

http://www.southerncrosscables.com/layup_ms19_8_02.htm

🔥 Emergency call-center power-supply woes

Dave Stringer-Calvert <dave_sc@csl.sri.com>

Mon, 19 Aug 2002 21:46:05 -0700

One of North Yorkshire Police's main telephone switchboards was shut down for four hours as the result of a serious control-room power-supply problem in Newby Wiske, Northallerton. Traffic was redirected to the York control room, which had considerable congestion due to the reduced total number of operators. [Source: Article by Tony Tierney, *Yorkshire Evening Press*, 19 Aug 2002; PGN-ed]

✶ YASST: Yet Another Silly Spam Trick

Rob Slade <rslade@sprint.ca>

Sun, 4 Aug 2002 14:58:43 -0800

At the moment I have a hotmail account, rmslade@hotmail.com. It gets a ton of spam, of course. Recently, as I was cleaning ou the accumulated sludge (Hotmail's "junk" settings are pretty useless), I noted a message that appeared to come from "rmslade." Now, it isn't unusual for spammers to set up the mailing so that the messages have a forged "From" line that contains the same address the message is sent to. Only in this case, the message was from rmslade@yahoo.com, and that is not an address I own.

Looking at the headers in detail revealed (along with the fact that the spammer is probably yallddamail.com [65.121.131.5] [Qwest Communications]) that the actual address used is \$user@yahoo.com.

Now, as I said, spammers spoof addresses all the time. But does Hotmail have to enable such a transparent means of allowing it?

rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

<http://victoria.tc.ca/techrev> or <http://sun.soci.niu.edu/~rslade>

✶ Re: E-mail content filtering ... (Miller, [RISKS-22.16](#))

Joe Stoy <stoy@sandburst.com>

Mon, 29 Jul 2002 10:32:34 -0400

My favourite story along these lines is about the two German musicologists who were having a learned discussion by e-mail about Bach's B Minor Mass, until both simultaneously came to the conclusion that the other side was losing interest towards the end of the Gloria. But it turned out that their e-mail system was simply refusing to let through any mention by name of the magnificent fugue at the end of that section.

✶ E-mail *envelope* filters blocking NDN and DSN

MAtteo HCE Valsasna <valsasna@uninsubria.it>

Mon, 29 Jul 2002 16:24:00 +0200 (CEST)

Many RISKS readers have already reported about RISKS associated with e-mail filters based on the contents. But serious service RISKS are also associated to envelope-based filters, i.e., filters based on the sender (or recipient) used in SMTP transactions (in contrast with those present in the e-mail headers).

Many SMTP servers have started filtering e-mail with an empty envelope sender, their administrators claiming they can block a lot of spam that way. This is in clear contrast with RFC [rfc1123, see quote below].

A reason for this is that an empty envelope sender must be used with NDN

(Non Delivery Notification) and DSN (Delivery status notification) messages, which are used to inform the sender that his message couldn't be delivered to the recipient, or to confirm to the sender the delivery or the reading of a message [rfc1891, see quote below].

Filtering those messages could mean that, under certain conditions, a delivery confirmation could fail to reach the sender, or, much worse, a non-delivery notification could never reach the sender.

When empty reverse path filtering is applied at the SMTP server receiving messages for the user's address, NDN and DSN messages originated at other servers will be rejected. This can happen for example if the user uses a different SMTP server to send her messages, if the SMTP server that receives a message does not reject it immediately, but rather accepts it and later generates a negative DSN message to inform the reader of the missed delivery, and also happens for DSN messages generated at a different domain than the sender's.

SMTP gives no guarantees about the delivery of a message, but makes any possible effort to inform the sender that a message could not be delivered (also these efforts are not generally guaranteed to succeed). Filtering messages with an empty envelope sender risks to render these attempts useless.

Users have got accustomed to receive a negative confirmation (NDN) when they send a message that will never reach the recipient, so they may

trust that a message for which they received no NDN has actually been delivered (a classical problem of double-negative logic). Filtering empty reverse path messages will void this trust, leaving the sender with the impression that his message has reached someone. The RISKS associated with this false assumption are obvious.

The assumption is actually false basing on SMTP's absence of guarantees, not on the improper loss of NDN messages due to empty smtp sender filtering, but users do not read manuals, they look at how the service actually works and build their assumptions accordingly.

Another general-purpose RISK (assuming that a system that usually works will *always* work).

MATteo HCE Valsasna - Network & Linux Administrator
Centro SIC - Univ. degli Studi dell'Insubria

<http://www.faqs.org/rfcs/rfc1123.html> (Requirements for Internet Hosts
-- Application and Support)

5.2.9 Command Syntax: RFC-821 Section 4.1.2

The syntax shown in RFC-821 for the MAIL FROM: command omits the case of an empty path: "MAIL FROM: <>" (see RFC-821 Page 15). An empty reverse path MUST be supported.

<http://www.faqs.org/rfcs/rfc1891.html> (SMTP Service Extension for Delivery Status Notifications)

7.1 SMTP Envelope to be used with delivery status notifications

The DSN sender address (in the SMTP MAIL command) MUST be a null reverse-path ("<>"), as required by section 5.3.3 of [9]. The DSN recipient address (in the RCPT command) is copied from the MAIL command which accompanied the message for which the DSN is being issued. [...]

⚡ Content based e-mail filtering -- timely example

Betsy Schwartz <betsys@pobox.com>
Sun, 11 Aug 2002 12:59:17 -0400

Another problem is that it's impossible for any one sysadmin to know, for a given string, whether it's a legitimate word or name in some contexts.

I've had several people say to me recently: "but, what legitimate e-mail could possibly contain the word 'klez' "? Well, I am a big fan of klezmer music and there will be some sad wedding parties if "klez" is filtered out!
See <http://www.klezmershack.com>

[And this will undoubtedly get THIS issue filtered for some readers. PGN]

⚡ Klez + html login = no security

Leonard Erickson <shadow@krypton.rain.com>
Tue, 20 Aug 2002 03:12:14 PST

I mostly use a DOS based mail reader program, so I often get MIME encoded mail or other mail that may or may not have viral payloads (or just typical Microsoft "everyone uses our mailer" dreck).

I move the messages to a directory to be checked out later.

Today I was going thru the message that'd piled up there over the last couple of weeks. And I was looking at the other files included in Klez infected messages.

One was a file that had "login" as part of the name, and no extension. A quick check with LIST showed it to be an HTML file. Out of curiosity, I added an HTML extension, and looked at it on a Windows system.

I found myself on a website for a company I won't name. With the username and password having just been entered on a login screen!

A password that seems to still be valid.

I found a "technical problems" email address on the web site and mailed the contact the info about the problem. And I deleted the file.

But whatever program created this login "file" (I think html had embedded Javascript) is **really** a bad idea to have in this world that has viruses that email random files from infected systems to the world.

Anybody care to bet that my report to the company gets ignored?

Leonard Erickson (aka shadow{G}) shadow@krypton.rain.com

✶ Klez: The Virus That Won't Die

Monty Solomon <monty@roscom.com>

Thu, 22 Aug 2002 09:15:25 -0400

Already the most prolific virus ever, Klez continues to wreak havoc.

By Andrew Brandt, Sep 2002 issue of *PC World* magazine, 1 Aug 2002

The Klez worm is approaching its seventh month of wriggling across the Web, making it one of the most persistent viruses ever. And experts warn that it may be a harbinger of new viruses that use a combination of pernicious approaches to go from PC to PC.

Antivirus software makers Symantec and McAfee both report more than 2000 new infections daily, with no sign of let-up at press time. The British security firm MessageLabs estimates that 1 in every 300 e-mail messages holds a variation of the Klez virus, and says that Klez has already surpassed last summer's SirCam as the most prolific virus ever.

And some newer Klez variants aren't merely nuisances--they can carry other viruses in them that corrupt your data. ...

<http://www.pcworld.com/news/article/0,aid,103259,00.asp>

✶ The left hand of the government asketh ...

Rob Slade <rslade@sprint.ca>

Thu, 1 Aug 2002 08:34:19 -0800

Despite the reports being a day apart, the following two stories appeared next to each other in last evening's Edupage from EDUCAUSE. EDUCAUSE made no comment on the juxtaposition. However, I suspect that pretty much anyone can see the cause for concern here. Poorly thought out "quick fix" legislative solutions, such as the DMCA, can definitely be much more trouble than they are worth.

----- Forwarded message follows -----

>Date sent: Wed, 31 Jul 2002 17:43:42 -0600
>From: EDUCAUSE@EDUCAUSE.EDU
>Subject: Edupage, July 31, 2002

[...]

TOP STORIES FOR WEDNESDAY, JULY 31, 2002

Clarke Urges Hackers to Find and Report Bugs
H-P Uses DMCA Against Bug Finders

[...]

CLARKE URGES HACKERS TO FIND AND REPORT BUGS

Richard Clarke, the cybersecurity advisor to President Bush, told attendees of the Black Hat conference in Las Vegas that they should find and report software bugs that compromise computer security.

[...]

Associated Press, 31 July 2002

<http://www.nandotimes.com/technology/story/484376p-3867743c.html>

H-P USES DMCA AGAINST BUG FINDERS

In an apparent first, Hewlett-Packard has invoked the controversial

Digital Millennium Copyright Act (DMCA) to stop researchers from releasing information about software bugs. [...] But H-P sent a letter to SnoSoft, a group of researchers, saying that the group

faces fines of \$500,000 and jail time for releasing information about a

bug in an H-P Unix application. SnoSoft said that they notified

H-P of
the flaw early enough that a patch should have been available
before
public disclosure of the bug. [...]
CNET, 30 July 2002
<http://news.com.com/2100-1023-947325.html>

[...]

EDUPAGE INFORMATION

To subscribe, unsubscribe, or change your settings, visit
<http://www.educause.edu/pub/edupage/edupage.html>

🔥 Re: Apple OSX and iDisk and Mail.app

Dave <davew1@mac.com>

Sat, 27 Jul 2002 21:08:50 -0400

from Volume 22 : Issue 18:

> Net effect: your iDisk password is transmitted in the clear
without

> your awareness, albeit as a mail password.

> Problems:

...

> - mac.com's mail password is **always** identical to iDisk
password

Yes, by definition. mac.com mail and iDisk are part of iTools
(now ".Mac")

which uses a single account/password to access all of its
services.

> - OSX's "do what I mean" friendliness saves passwords without
knowledge

Users enter their iTools info in the Internet preferences panel
which

states: "Enter your member name and password. This information

is used to
access iTools, including your iDisk and your e-mail account."
Hard to
misinterpret that.

> then connects to mac.com which *does not* support any method of
> encrypted password transmission.

That's the real problem which Apple will correct quickly (right
guys?)

REVIEW: "Computers and Ethics in the Cyberage", Hester/Ford

Rob Slade <rslade@sprint.ca>
Tue, 20 Aug 2002 15:12:27 -0800

BKCMETCB.RVW 20020606

"Computers and Ethics in the Cyberage", D. Micah Hester/Paul J.
Ford,
2001, 0-13-082978-1, U\$41.00
%A D. Micah Hester
%A Paul J. Ford
%C Scarborough, Ontario
%D 2001
%G 0-13-082978-1
%I Prentice Hall
%O U\$41.00 800-576-3800 416-293-3621 fax: 201-236-7131
%P 498 p.
%T "Computers and Ethics in the Cyberage"

This volume is a collection of essays, arranged in a rather
complex fashion.
There are parts, subdivided into chapters, with each chapter
containing
about four papers. It isn't necessarily difficult to find the
theme running
through each set of papers, but neither does the conjunction of
ideas

support the individual discussions.

The preface, interestingly, states that the book provides no general introduction to ethics. There are also lists of alternative orderings and selections of the papers included in the volume, suggested to address additional topics.

Part one is an introduction to technology, computers, and values which last is rather in contradiction to the assertion that the work contains no such introduction. In any case, there is no introduction to values. The essays in chapter one look at how the machine affects personality (a poetic but unconvincing piece), a review of various (both positive and negative but primarily religious) views of technology, opinions on technology and moral responsibility, and the ethical problems presumed to be unique to computers. Chapter two views computer technology as value-laden. The first paper insists that computers should be improved by the addition of abilities for responding to simple requests in natural language, apparently implying that the search for the "user-friendly" chimera has an ethical driver. (A common desire, but one that flies in the face of user-interface research that indicates people are, in fact, unable to frame requests accurately even in natural language.) Others assert that computers fail to distinguish between numbers and data (and between information and reason), that work with Boolean algebra molds the thinking process, and that computers are fun because they are magic.

Part two purports to review computers and quality of life.

Chapter three

looks at technology and relations with other people. One paper points out

that the attitude of the Amish towards the telephone is supportive of

community living, but admits that the example has almost no relation to

other technology. Others discuss various things you can do online, how much

Howard Rheingold likes the WELL service, and that John Perry Barlow doesn't

know whether community actually exists (online or in real life). Computer

and individuality is addressed, in chapter four, with an unsupported

assertion that technology has some normative value, wild speculation on

implantable brain chips, a fictional short story about artificial personality, and vague thoughts about the anthropomorphizing effect of the

changing language with regard to computers. A look at computers in

developing nations assumes that the purpose of computer use is control,

asserts (but does not support) the idea that western (and therefore somehow

"authoritative") computers are unsuited to Africa (the entire continent is

assumed to have unreliable data), that information technology can help in

Latin America but there are problems, presents random memories of email use

in Jamaica, and asserts, in chapter five, that transferring technology to

the third world can create problems.

Part three concentrates on the uses, abuses (and maybe consequences) of

technology. Chapter six looks at professionals and ethics, with various

views of whether professions have special obligations (and a

final decision
that computing is not a profession), scenarios emphasizing
conflicting
loyalties, and some factors that might help reduce computer
misuse.
Freedom, privacy and control is the topic of chapter seven,
discussing
problems with direct democracy, reprinting a political speech
nominally
about privacy, and attempting to determine a definition and some
characteristics of privacy. A review of intellectual property
ownership and
piracy has an interesting examination of the differences in
attitudes to
copyright between western (stressing ownership and roles) and
Asian
(emphasizing social benefits and outcomes) cultures, as well as
a student
survey, a statement that the arguments in favour of copyright
are at best
unproven, and an opinion promoting copy protection cracking and
the
distribution of "cracked" commercial programs (with the usual
lack of logic
and writing skills). (Despite this last essay, chapter eight is
possibly
the best in the book.) Chapter nine has some sensationalistic
material on
hacking (and a very poor introduction to viruses) with no real
conclusions,
a hacker "manifesto," a strong (but no perfect) analysis
deciding that
computer intrusions cannot be held to be "victimless," an
interview with a
self-styled "hacker" (as self-serving as most such), and a weak
examination
of the Morris Worm.

Part four seems to assume that it is moving into more advanced
or futuristic
technologies, although the discussions don't change much.
Chapter ten has
another fictional short story implying that computers are false

gods, a
replay of "What Computers Can't Do," and a vague wondering about
the
definition of life. One essay, very much in contradiction to
the thesis of
Rosalind Picard's excellent "Affective Computing" (cf. BKAFFCMP.
RVW)
maintains that a computer which is "superior in every way" (to
us) must be a
"monster," and assumes that artificial intelligence will be
devoid of
compassion. (Even if one does accept that intelligence must be
emotionless,
there is no mention of the fact that such a system would also
lack cruelty.)
The overview of virtual reality (VR) has an interesting
examination of the
health and safety effects (limited) and benefits of the
technology, and two
assertions of the need for a VR ethic, in chapter eleven. In
chapter
twelve, Al Gore sells the GII (Global Information
Infrastructure), we are
told that there is pornography on the Internet, Dibbell's
classic "Rape in
Cyberspace" is reprinted, and an article on cyberstalking seems
to void its
premise by repeatedly demonstrating that most of the activities
take place
in the real world, not the net.

Many of the papers in this collection are lifted wholesale from
their
origin. Although ellipses seem to indicate that material has
been cut in a
number of places, there are still some very odd references to
other papers
or presentations no longer "present," and even comments directed
at people
who are no longer in the audience.

Much of this material is quite seriously flawed by a lack, on
the part of

the authors, of a technical background. This is not to say that non-technical people cannot comment on the social aspects of technology, nor that discussions of technical ethics could not benefit from the input of philosophers, ethicists, sociologists, and the like. However, many of the speculations bear little relationship to technical reality, and therefore the arguments and decisions are invalid.

Overall, there is a lack of direction to the work. In the end, it gives an impression of a vague complaint that computers aren't moral, and aren't taking the burden of ethical decisions away from mankind. Personally, I find this position not only unhelpful, but extremely odd.

copyright Robert M. Slade, 2002 BKCMEVCB.RVW 20020606
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

<http://victoria.tc.ca/techrev> or <http://sun.soci.niu.edu/~rslade>

✶ SAFECOMP 2002 & ECCE-11

Massimo Felici <massimo.felici@ed.ac.uk>
Tue, 20 Aug 2002 18:30:11 +0100

SAFECOMP 2002
The 21st International Conference on
Computer Safety, Reliability and Security
Catania, Italy, 10-13 September 2002, Catania, Italy
<http://www.safecomp.org/>
contact safecomp2002@safecomp.org

Co-located and Coordinated with

ECCE 11 - Cognition, Culture and Design
Eleventh European Conference on Cognitive Ergonomics
Catania, Italy, 8-11 September 2002
<http://www.ecce.info/>



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

[ACM](#) Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 21

Tuesday 27 August 2002

Contents

- [VeriSign error teaches lawyer a lesson](#)
[Max](#)
- [Automation increases anxiety -- with cause](#)
[Fuzzy Gorilla](#)
- [Big Brother hiding inside cars' airbags](#)
[Monty Solomon](#)
- [Keystone SpamCop summary and response](#)
[Edward W. Felten](#)
- [SpamAssassin killed off RISKS-22.20](#)
[Danny Burstein](#)
- [Re: "Homeland Insecurity"](#)
[Stephen Fairfax](#)
- [Re: Your packets know the way to San Jose](#)
[Barry Margolin](#)
[Steve Wildstrom](#)
[Gene Wirchenko](#)
[R.G. Newbury](#)
- [Re: YASST: Yet Another Silly Spam Trick](#)
[Tai](#)
- [Re: Klez: The Virus That Won't Die](#)
[Excimer](#)

[Scott Peterson](#)

● [REVIEW: "Access Denied", Cathy Cronkhite/Jack McCullough](#)

[Rob Slade](#)

● [Info on RISKS \(comp.risks\)](#)

✶ **VeriSign error teaches lawyer a lesson**

Max <max7531@earthlink.net>

Sun, 25 Aug 2002 08:16:20 -0700

Fremont, California, attorney Anu Gupta's Web site www.immigrationdesk.com was mistakenly transferred to a company in India, as the result of an error by VeriSign. (She helps people get visas, green cards and other documents.)

After five days of haggling with VeriSign, Gupta eventually regained control of the site, but only after she threatened to sue. E-mail sent during that time disappeared, and could have included credit card and tax information.

[Source: Lawyer learns hard lesson on wild, wild Web, Peter Delevett, *San

Jose Mercury News*, 25 Aug 2002; PGN-ed]

<http://www.bayarea.com/mld/mercurynews/news/local/3935313.htm>

From the article: VeriSign has garnered a reputation for shoddy customer service and questionable marketing. A federal court ruled in June [2002] that the company had poached competitors' customers by sending them bogus renewal letters, and several related lawsuits are pending. The Federal Trade Commission is also investigating VeriSign's marketing. ... The real pity for Gupta and other disgruntled Internet users is that there's no enforcement body standing up for them.

Automation increases anxiety -- with cause

"Fuzzy Gorilla" <fuzzygorilla@euroseek.com>

Sat, 24 Aug 2002 12:19:00 -0400

People are often worried about computerization for a good reason. Even though it is the same information, the potential risks from abuse are increased. Black lists, blackmail, and sending private information to the wrong parties were all reported. [FG]

There is considerable controversy in Japan at the moment over an attempt to put personal information on-line in a family-registry database, along with an 11-digit identifying number for everyone. In addition to fears relating to hackers and criminals, "one of their chief concerns is misuse of the data by their own government." Polls show huge majorities are against the system. [Source: Plans to Computerize Personal Data Ignite Firestorm in Japan; Citing Privacy, Municipalities Defy Effort By Doug Struck, *The Washington Post*, 23 Aug 2002, A18; PGN-ed]

<http://www.washingtonpost.com/wp-dyn/articles/A51216-2002Aug22.html>

From the article:

There is plenty of grist for public suspicion of bureaucrats. In May, the Defense Agency admitted it had drawn up a list with names, backgrounds and

political views of citizens who had asked for public information from the agency. Twenty-nine agency officials were punished. Last month, defense contractor Fujitsu said it had gotten a blackmail demand from men who had obtained personal information on military officers leaked from the company's computers. And just as Juki Net started up, embarrassed officials in the city of Moriguchi in Osaka acknowledged they had sent personal information about 2,584 individuals to the wrong people.

✶ Big Brother hiding inside cars' airbags

Monty Solomon <monty@roscom.com>

Thu, 22 Aug 2002 19:09:12 -0400

On 11 Feb 2002 on Union Road in Trotwood, Ohio, a 1999 Pontiac Trans Am skidded sideways off the road, went airborne for 110 feet, and eventually hit a utility pole. An estimate of the car's speed was upgraded after examining an onboard electronic monitoring device in the airbag control mechanism, which pegged the speed at 124 mph (in a 40-mph zone). [Source: *Dayton Daily News*, By Cathy Mong, cathy_mong@coxohio.com; PGN-ed]

<http://www.activedayton.com/ddn/local/0822car.html>

✶ Keystone SpamCop summary and response (Re: [RISKS-22.19](#))

"Edward W. Felten" <felten@CS.Princeton.EDU>

Mon, 26 Aug 2002 11:45:27 -0400

[HTML version (same text, but somewhat easier to read) available at

<http://www.freedom-to-tinker.com/archives/000023.html>]

I received 59 responses to my SpamCop narrative. Because there are so many, I cannot respond individually to each one. Instead, I summarize below the major arguments raised by the messages. I give sample text from messages that asserted each argument, and I respond.

This posting is rather long, and some readers may not be interested in the whole thing, but I think the people who sent me constructive messages about the SpamCop incident deserved a response.

Argument 1: Blame the ISP, not SpamCop.

Sample:

"The problem is not with Spamcop, but rather with your ISP. The ISP is required to assert that they have dealt with the issue, not that they have shut the website down. They can mark the issue 'resolved' with spamcop and then work with you to discover the true nature of the problem. The choice to shut the web site down now, and investigate later, was your ISP's, not Spamcop's. "

Another sample:

"However, in this case, your ISP is responsible for bouncing your domain, not SpamCop. All SpamCop e-mails come with a link to the original report, so it was your ISP who failed to research this and your ISP who is to blame for suspending your site."

My response: Certainly my ISP is the party who actually pulled the plug on my site. The ISP was intimidated by SpamCop and seemed to be trying to show that it was responsive to SpamCop complaints. Hence the quick shutoff of my account.

Yet even after I convinced my ISP that I was not a spammer, they still refused to reinstate my site, saying that to do so before SpamCop removed the complaint against me from its site would put the ISP's other customers at risk. This refusal to reinstate my account is what convinced me that the ISP was afraid of SpamCop.

Whether the ISP was right to fear SpamCop, I cannot say. What I know is that the ISP chose to anger a paying customer, rather than risking what they perceived as the wrath of SpamCop. The fact that SpamCop engenders such fear is a big part of the problem. For me, the bottom line is this: if SpamCop didn't exist, my site would not have been shut off.

Argument 2: SpamCop doesn't block sites, ISPs block sites.

Sample:

"SpamCop (<http://www.spamcop.net>) blocks nothing. SpamCop does have a DNS-based blackhole list that ISPs have the option of using---for example, I use it for all my domains as a backup to my own block list."

Another sample:

"The spamcop blacklist is supposed to be used in order to tag certain email as possible spam. It is not to be used to block email (although

some ISP's do use it that way)."

Another sample:

"ISPs also use Spamcop, but it is the ISP, not Spamcop, that makes the determination whether something listed by Spamcop is deleted, flagged, or passed through. I happen to delete."

My response: Nearly everybody who made this argument followed it by saying that they themselves do automatically block sites on the block list, or that many others do. This is hardly surprising. Even a perfect block list would do little good unless people used it to block. The alternative use of shunting aside email from sites on the list, and reading it later, doesn't do much to address the spam problem. As far as I can see, there are only two sensible things to do with a block list: you can ignore the list, or you can use it to block sites.

That's why they call it a "block list." That's why SpamCop's site gives instructions for configuring common mail servers to block addresses on the list. SpamCop can hardly be surprised to see ISPs following these instructions and blocking the addresses on what SpamCop itself calls a "block list."

Argument 3: SpamCop is just a clearinghouse for spam complaints and simply routes complaints that could have been sent even in the absence of SpamCop.

Sample:

"SpamCop is a machine. It summarizes and reports what human individuals feed it.

Another sample:

"SpamCop is primarily a `_reporting_` service which allows a user to easily report email abuse to the appropriate authorities. It has a parser which cracks email header information and figures out the true source of the email (as much as possible) despite forged header information.

This is just the same as manually email[ing] a complaint, but automates the header analysis (which can save a lot of time when the headers are intentionally obfuscated).

A user does not 'send an accusation to SpamCop' but uses SpamCop to email a complaint to abuse or postmaster addresses."

My response: SpamCop does more than just forward complaints. It anonymizes the complainant's address, thereby making it harder for the ISP receiving the complaint to judge the complaint's credibility. SpamCop puts the complaint on the Web for others to see. And SpamCop tries to find patterns among its complaints, and adds addresses to its block list based on these patterns. All of these factors contributed to my dilemma.

If SpamCop were merely a complaint router, then SpamCop would be ineffectual. It is SpamCop's "value added" that caused me trouble.

Argument 4: Blame the person who erroneously reported the

"spam," don't
blame SpamCop.

Sample:

"The SpamCop user, not SpamCop itself, is ultimately responsible for what is sent. Each report has been individually submitted by a user, then individually selected by the user before sending."

Another sample:

"The 'mistaken' reporter of spam violated SpamCop's terms of service, period. It doesn't matter if you call 911 to report a fire or a burglary: at the end of the day, individuals are responsible for their reporting, the telephone company is not to be blamed for prank calls to 911."

My response: This is really just a variant of Argument 3, and fails for the same reasons.

SpamCop is ultimately responsible for its reporting, too. The 911 analogy doesn't apply, since the phone company merely receives the report but SpamCop repeats reports and amplifies them. SpamCop took what would otherwise have been a private report, to be dealt with between the reporter and my ISP, and posted it for the whole world to see. And it gave the report increased credibility and force.

Argument 5: The attributes of SpamCop that Felten complained about are necessary to prevent spam, or to prevent retaliation by spammers.

Sample:

"In the absence of anti-spam laws with teeth, technical[ly] shunning ISPs who deliberately harbor spammers is the only alternative to control spam."

Another sample:

"[SpamCop anonymizes the complainant's address because] real spammers might take action against a spam reporter, such as using their address as the 'From' on a spam run."

My response: Yes, SpamCop's designers had good intentions. Yes, effective spam-fighting was their goal. My point is that in their zeal to fight spam, they built a system that overreacts to erroneous or malicious spam reports. I for one would not be willing to accept that kind of collateral damage, even if doing so would completely prevent spam (which it cannot).

Several people said that SpamCop is slower to act against accused parties than some other anti-spam services are. That may well be true.

If it is, then the other services are presumably causing even more collateral damage.

Argument 6: Felten really is a spammer.

"[Quoting Felten:]'Never mind that I had never sent a single e-mail message from the site.'

Reply: Someone did:

Mail for freedom-to-tinker.com is handled by freedom-to-tinker.com (0)

209.51.158.242

<http://www.sampade.org/t/dns?a=freedom-to-tinker.com>

If you look here, you will see two different headers that came from this

IP address, both of which are dated July, 31:

<http://spamcop.net/w3m?action=checkblock&ip=209.51.158.242>

Those are only examples; there could have been many more spams reported through that address."

My response: I did not send those messages. The writer apparently believes that if the messages came from "my" IP address, then I must be responsible for them. But it's not my IP address -- it's shared by many of my ISP's customers. Perhaps the cited messages came from one of them.

This argument nicely illustrates the problem with SpamCop. By collecting complaints in one place and indexing them, SpamCop facilitates the making of this kind of accusation. And by repeating allegations made by others, SpamCop gives them more credibility than they deserve.

✶ SpamAssassin killed off [Risks Digest 22.20](#)

danny burstein <dannyb@panix.com>

Thu, 22 Aug 2002 21:44:29 -0400 (EDT)

I run SpamAssassin ([RISKS-22.08-10](#)) using the default settings. (I push tagged mail aside into a spam box for leisurely review so I'm

not too
worried about false positives.)

It didn't like the latest issue of RISKS. Meaning, alas, that if people are using SpamAssassin to reroute (suspected) spam to the trash pile, or worse, if the ISP is using it ahead of the subscribers, many copies never got to the intended recipient.

✉ **Re: "Homeland Insecurity" ([RISKS-22.20](#))**

Stephen Fairfax <fairfax@mtechnology.net>
Thu, 22 Aug 2002 20:05:10 -0400

Mann's article ([RISKS-22.20](#)) is indeed timely and well-written, but with all due respect to both Mann and Bruce Schneier, I believe they miss some important points.

It's fine to suggest that systems fail smartly, or well, or not be brittle, but often designers are limited in choosing how systems fail. Complex systems have an annoying habit of exhibiting new and unforeseen failure mechanisms. Ultimately the failure mode is determined by laws of physics (for machines) or human behavior and are not easily controlled. That isn't to say that one can't select the most robust method of mitigating the consequences of failure, but practically speaking, the options are often quite limited.

What is not so severely limited, and what I feel is largely absent from the present approaches to security, is formal, quantitative analysis of what happens AFTER the first failure. My company applies the techniques of Probabilistic Risk Assessment (PRA) to high-reliability power systems for data centers, banks, hospitals, etc. There are many lessons to be learned, but one of the most important is that of layers. Once you understand that a particular failure can occur, you examine its consequences and make an informed choice about whether the system should be designed to continue functioning after that failure. If so, you generally need to add either redundant components, or some new system to handle the failure. In both cases, you need to take care that the cause of the initial failure is unlikely to compromise the response.

One can take advantage of knowledge of the system state after the failure in designing the next layer of protection. For example, if utility power fails, you can use the fact that most outages are brief, less than a few minutes, to rely on battery back-up rather than immediately starting standby engine-generators. This saves wear and tear on the engines, and helps one to select the appropriate discharge time rating for the batteries. If the outage lasts more than 2 minutes, the engines are started, and now the operators know that the outage is likely to last at least 30 minutes or longer, and can plan their actions accordingly.

PRA formalizes and quantifies this kind of thinking. Applied to

the problem of airport security, it offers a way to evaluate the effectiveness of various proposals. It doesn't take much analysis to show that successive "random" screenings, using the same tools, techniques, and personnel as the original, 100% screening of passengers, adds essentially zero value. (Aside: I always ask to see the dice, and never have. RISKS readers know full well the process is not random, but merely a concealed method of selection.) On the other hand, a targeted screen, applied after the 100% initial screen, by specially trained individuals, and using different methods (such as pointed, face-to-face questioning, as practiced by some non-US airlines) can yield large improvements. You can trade off the training and tools applied to the initial screen and the secondary screen to get the best result for a given level of investment.

Nearly all security analysis seems to ignore or completely discount the actions of lawful passengers after security failures, but the examples of Flight 93 and the apprehension of the would-be shoe-bomber suggests that this layer of defense is very robust and surprisingly capable. The "good guys" vastly outnumber the "bad guys," our thinking should take advantage of that fact!

Guns in the cockpit represent an independent layer that does not automatically fail when screens fail. While there is heated debate about the possibilities of negative consequences, a dispassionate analysis of the probabilities of both success and failure offers rather overwhelming

evidence that on balance, armed pilots will reduce both the likelihood and consequences of hijacking attempts.

In summary, while it is certainly important to have systems fail gracefully when possible, it is not always possible. That does not excuse the architects of security systems from performing careful, quantitative, reviewable analysis of their designs. Like cryptography, public review and discussion of the algorithms used in truly well-designed security systems will not compromise their integrity.

Stephen Fairfax, President, MTechnology, Inc., 2 Central Street
Saxonville, MA 01701 1-508.788.6260 fairfax@mtechnology.net www.
mtechnology.net

✂ Re: Your packets know the way to San Jose (Purvis, [RISKS-22.20](#))

Barry Margolin <barmar@genuity.net>
Thu, 22 Aug 2002 23:08:41 GMT

I think they may be overestimating how much traffic goes through MAE-West.

All Tier-1 ISPs have private peering interconnects, we don't use any of the public peering points to exchange data with each other. I don't have any statistics to back me up, but I expect that most Internet traffic goes through these private interconnects, not the public ones, which are used for connections to and between smaller ISPs.

Also, MAE-West is just one of several public peering points in the continental US, and nationwide backbones usually connect to each other using at least two (we make that a requirement of all our peering partners -- an ISP that can't meet our criteria has to purchase normal ISP service from us, rather than being a peer).

Destroying that building would certainly have an impact on the Internet, as all its traffic would have to be rerouted, and would cause congestion at the other interconnects. For the most part, this would happen automatically (I qualified this, because some ISPs have misconfigured routers, so they don't advertise all their routes at all the exchange points), although it would probably take several minutes to stabilize.

To deal with the congestion at the other exchanges, I expect that most of the Tier-1's would relax their transit rules, so that some of it would be shunted to those private interconnects I mentioned earlier. We did similar things last year in the wake of 9/11.

Barry Margolin, barmar@genuity.net, Genuity, Woburn, MA

✶ Re: Your packets know the way to San Jose (Purvis, [RISKS-22.20](#))

Steve Wildstrom <steve_wildstrom@businessweek.com>
Thu, 22 Aug 2002 20:44:11 -0400

MAE West is only the beginning. There are also MAE East, MAE Central, MAE Chicago, MAE Los Angeles, MAE Paris [MAE OUI?], and MAE Frankfurt -- all owned and operated by WorldCom.

I've been surprised by how little public discussion there has been about the amount of critical infrastructure controlled by WorldCom. Should we be very afraid? I know that WorldCom is operating more or less normally under bankruptcy protection and it is in the interest of the creditors that the Internet business remain alive as a going concern, but still, it is a dangerous and potentially very unstable situation. At a minimum, there isn't going to be any investment in these facilities at least until the future of WorldCom is decided. Given the fact that potential buyers can't perform due diligence until the auditors get to the bottom of the accounting mess, the uncertainty could last a long time.

Steve Wildstrom Technology & You Editor Business Week
1200 G St. NW Suite 1100 Washington DC 20005 1-202-383-2203

★ Re: Your packets know the way to San Jose (Purvis, [RISKS-22.20](#))

Gene Wirchenko <genew@mail.ocis.net>
Fri, 23 Aug 2002 03:31:33 GMT

> also see that MAE West is owned by WorldCom.

^

I think you left out "partly", Mr. Purvis.

At the bottom of it is "Southern Cross is owned by Telecom New Zealand (50%), Optus (40%) and Worldcom (10%).".

^^^

That is just a bit different, no?

⚡ Re: Your packets know the way to San Jose (Purvis, [RISKS-22.20](#))

"R.G. Newbury" <newbury@mandamus.org>

Thu, 22 Aug 02 21:26:04 -0500

IIRC, MAE East is part of a parking structure.... You can drive up and park next to it.. I suspect it would not take more than a Volkswagen Beetle sized car b*mb to inflict major disruption.

Do you think that **anyone** in the "intelligence business" (yes, I **know** that that is an oxymoron) is worrying about the security of this portion of the Internet???

⚡ Re: YASST: Yet Another Silly Spam Trick (Slade, [RISKS-22.20](#))

Tai <tai@fedex.com>

Fri, 23 Aug 2002 09:26:25 +0000

My wife is convinced that hotmail is a spammer. She created an account that was never given out, and received spam all the time. 6 months later, so

forgot the password, and created another account. This account does not receive spam at all.

The difference? The first acct belonged to a .usian with .us zip codes, etc. The second acct had an address in some third world country, ie, not .us based.

✶ Re: Klez: The Virus That Won't Die ([RISKS-22.20](#))

<Excimer3@aol.com>

Fri, 23 Aug 2002 13:15:30 -0400

Viruses are becoming more sophisticated, we know that. We also know that they will get worse as they become more and more advanced. Here's a thought: Imagine a Klez descendant with a small distributed-computing payload. Each infected system becomes a node in a neural net. This net would be slow, and the nodes would come and go, but it would be immense and uncontrollable. The possible implications are scary. Science fiction becomes science fact.

✶ Re: Klez: The Virus That Won't Die ([RISKS-22.20](#))

Scott Peterson <scott4@mindspring.com>

Thu, 22 Aug 2002 22:00:12 -0700

Maybe the even bigger irony is that Microsoft released a patch for Internet Explorer that stops KLEZ dead in its tracks in March, 2001. It's also included in current service packs for it.

<http://www.microsoft.com/technet/security/bulletin/MS01-020.asp>

★ **REVIEW: "Access Denied", Cathy Cronkhite/Jack McCullough**

Rob Slade <rslade@sprint.ca>
Thu, 22 Aug 2002 10:06:22 -0800

BKACCDEN.RVW 20020604

"Access Denied", Cathy Cronkhite/Jack McCullough, 2002, 0-07-213368-6,
U\$24.99

%A Cathy Cronkhite

%A Jack McCullough

%C 300 Water Street, Whitby, Ontario L1N 9B6

%D 2001

%G 0-07-213368-6

%I McGraw-Hill Ryerson/Osborne

%O U\$24.99 905-430-5000 800-565-5758 fax: 905-430-5020

%P 283 p.

%T "Access Denied: The Complete Guide to Protecting Your
Business
Online"

The introduction states that business leaders often lack the background to deal with technical security issues, and that the book seeks to fill the technical gap. Ordinarily I am wary of such claims, particularly in such slim volumes, but, after a poor start, this one works

surprisingly well.

Chapter one concentrates on "hackers." There is sensationalism, and there are errors, such as confusing Clifford Stoll's "wily hacker" with members of the Chaos Computer Club, but the text does at least divide security breakers into various camps, rather than lumping them all together. The discussion of viruses and malware, in chapter two, is the all-too-common unreliable mix of errors (the "Cokegift" prank is stated to be a virus) and reasonable material. A random collection of email dangers and netiquette makes up chapter three. Another miscellaneous list of Internet attacks and some misinformation (a discussion of "poisoned" cookies) is given in chapter four, but no means of protection.

After this, however, the book improves. The review of encryption, in chapter five, is a clear presentation for the non-specialist. Chapter six is a reasonable guide to backup. Network security loopholes, and means of protecting them, are in chapter seven. Physical security is covered in chapter eight. Chapter nine looks at remote, wireless, and cellular security. Intrusion detection and documentation (suitable for presentation to law enforcement) is in chapter ten. The material on risk analysis, in chapter eleven, is slightly facile, but is a good accompaniment to policy development.

The subtitle slightly overstates the case in terms of completeness, but this work certainly is worthy of review by any manager without a

technical

background, who nevertheless needs to make decisions about security.

copyright Robert M. Slade, 2002 BKACCDEN.RVW 20020604

rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca

pl@canada.com

<http://victoria.tc.ca/techrev> or <http://sun.soci.niu.edu/~rslade>



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 22

Friday 30 August 2002

Contents

- [Real risks of cyberterrorism?](#)
[Chris Norloff](#)
- [Rookie's mistake melted down \\$500,000 transformer](#)
[Scott Wlaschin](#)
- [Police dispatch disrupted by broken lightbulb](#)
[Gene Berkowitz](#)
- [Sabotage in a few clicks: NDS vs. Canal Plus](#)
[Max](#)
- [Tough EU privacy rules influence U.S. Web practices](#)
[NewsScan](#)
- [Big Brother hiding inside cars' airbags - tells fibs](#)
[Bernd Felsche](#)
- [FEC OK's SMS spam without saying who paid for it](#)
[Hal Murray](#)
- [Website Security Flaw Costs ZD](#)
[Monty Solomon](#)
- [Transport worker ID in works; privacy rights, funding at issue](#)
[Monty Solomon](#)
- [The EUR-RVSM safety case is flawed](#)
[Peter B. Ladkin](#)

- [Bogus Probabilistic Risk Assessments](#)
[Peter B. Ladkin](#)
 - [Japanese phones vulnerable to hackers?](#)
[Monty Solomon](#)
 - [Microsoft warns of Office and IE risks](#)
[PGN](#)
 - [Computer expert says he can break Microsoft security](#)
[Monty Solomon](#)
 - [A better approach to spam](#)
[John Pettitt](#)
 - [Re: Keystone SpamCop summary and response](#)
[Crispin Cowan](#)
 - [Parody and copyright](#)
[Terry Carroll](#)
 - [Re: American style cyber warfare ...](#)
[Peter Hanecak](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Real risks of cyberterrorism?

"Chris Norloff" <cnorloff@norloff.com>

Thu, 29 Aug 2002 09:11:33 -0400

The article "What are the real risks of cyberterrorism?"

<http://zdnet.com.com/2100-1105-955293.html>

plays down risks from hostile access through Internet connections. The

conclusions seem to be based on a recent study by the Gartner Group and the

US Navy War College. This study, however, is not referenced or included.

Some statements from people apparently interviewed by the article's author

or perhaps were part of the Gartner/Navy study seem like something right out

of the RISKS archives:

Ellen Vancko, a representative for the North American Electric Reliability Council, said such access [direct access by Internet or modem]

should not always be considered unsafe. "All the electric companies are

connected to the Web in one way or another," she said. "But that doesn't

mean our control systems are hooked up to the public Net."

I'd like to hear what other RISKS readers think of the real risks of

"cyberterrorism" and poorly-protected supervisory control and data

acquisition (SCADA) devices.

[The report of the Clinton Administration's President's Commission on

Critical Infrastructure Protection (The Marsh Commission) ([RISKS-18.89](#),

[RISKS-19.43](#), [RISKS-19.61](#)) clearly indicated that essentially all of the

critical infrastructures had serious potential vulnerabilities. PGN]

⚡ Rookie's mistake melted down \$500,000 transformer

"Scott Wlaschin" <scott@extractofmalt.com>

Fri, 23 Aug 2002 19:21:31 -0700

Palm Beach Post, 23 Aug 2002 (via Romensko's Obscure Room)
http://www.gopbi.com/partners/pbpost/epaper/editions/friday/news_d3568ba0e56222b00057.html

With the flick of the wrong switch, an unsupervised power-plant apprentice melted down a half-million-dollar transformer, blacking out the

city for 40
minutes.

Apparently, Coady [the apprentice] failed to follow procedures.

Two circuit breakers -- called the east and west buses -- must be flipped in a particular order to avoid damaging equipment: the west bus first, then the east bus. The procedure was written for an important reason -- because the west bus turns on the cooling system for the transformer.

The switches are in separate rooms. Coady said he closed the east switch before Stephenson [the supervisor] closed the west one. They couldn't see each other when the [switches were closed and the] damage was done.

The result was disastrous. "It was literally an explosion inside the transformer," Lake Worth Utilities Director Miller said. "The internal parts of the transformer reached such high temperatures that even the insulation inside the transformer was burned."

Stephenson said Coady had no clue what had happened. "He was completely unaware," Stephenson wrote in a memo to Baker. "With his lack of knowledge of the plant electrical controls, it was not even possible to explain to him what he did. He would not have understood. His training did not include these advanced concepts."

// Comment:

Giant circuit breakers have to be flipped in a certain order blindly in different rooms? This was an accident waiting to happen. It is scary that

systems like this can exist. Note that the poor trainee was blamed, of course, for not understanding the 'advanced concepts'.

✶ Police dispatch disrupted by broken lightbulb

"Gene Berkowitz" <geneb.ma.ultranet@rcn.com>

Sun, 28 Jul 2002 20:10:35 -0400

This is a Rube Goldberg sort of story: Man damages cruiser. Police use pepper spray, restraints, place him in a cell. He jumps up and hits the cell light and microphone, destroying the light, tripping a circuit breaker, causing the dispatch room lights to go out and messing up the phone systems -- which still were not working properly the next day. [Source: Stacey Hart and Michael Wyner, *Sudbury Town Crier* (Massachusetts), 24 Jul 2002; heavily PGN-ed] <http://www.townonline.com/metrowest/sudbury/38116472.htm>

✶ Sabotage in a few clicks: NDS vs. Canal Plus

Max <max7531@earthlink.net>

Thu, 29 Aug 2002 06:10:22 -0700

Canal Plus (a maker of smart cards) alleges a rival firm (NDS Group, a competing company largely owned by Rupert Murdoch's News Corp) broke its secret code, then gave it to counterfeiter. (In Italy, for

example, 75% of premium-channel viewers are reportedly freeloaders using bogus cards.) Canal Plus is suing for a billion dollars in damages. NDS denies the charges, attributing the suit to "an attempt by an inept competitor to shift the blame for its incompetence." This situation has also played a role in the downfall of Vivendi's Jean-Marie Messier and the auctioning off of Vivendi's Italian satellite system -- purchased by News Corp. "The case marks the biggest and most sensational accusation yet of corporate cybercrime, a shadowy, unsavory and increasingly popular activity." [Source: A very long and interesting article by David Streitfeld, *Los Angeles Times*, Column One, 29 Aug 2002; PGN-ed]

Streitfeld's article also notes that "Seven years ago, Cadence Design Systems, a maker of design software for integrated circuits, sued Avant Corp., claiming it had stolen its programs. A subsequent criminal case, brought by a determined San Jose prosecutor, led to verdicts last year against seven current and former Avant employees, including the chief executive and three founders. Five received jail sentences."

Also, "In 1999, Internet bookseller Alibris paid \$250,000 to resolve federal charges that it had unlawfully intercepted thousands of e-mail messages to its customers from online bookseller Amazon.com."

⚡ Tough EU privacy rules influence U.S. Web practices

"NewsScan" <newsscan@newsscan.com>

Fri, 30 Aug 2002 08:38:06 -0700

Europe's strict approach to consumer data protection is forcing many U.S.-based companies to follow suit in order to continue serving their European customers. "Europeans are extremely concerned about the use of data about people," says Rockwell Schnabel, the U.S. ambassador to the European Union. "The data privacy issue is a huge issue over there. American partners have to live with those rules, and they can't do with it what they can with American data." A case in point is Microsoft's Passport online ID service that enables users to log in once and then move from one secure Web site to another. Consumer and privacy groups had accused Microsoft of not taking adequate steps to protect consumers' personal information and in a settlement earlier this month, Microsoft admitted no wrongdoing, but agreed to government oversight of its consumer privacy policies for the next 20 years. A separate Passport investigation by the EU is still pending. "The EU directive raised the bar on the practices by U.S. companies for U.S. consumers," says Marc Rotenberg, head of the Electronic Privacy Information Center. "Passport is a good example of that, because Microsoft is very much aware that its products are going to have to meet EU privacy standards." EU standards specify that data may be collected only for "specified, explicit and legitimate purposes, and to be held only if it is relevant, accurate and up to date." Citizens may access any data

about

themselves, find out its source, correct inaccuracies, and pursue legal recourse for misuse. [*San Jose Mercury News*, 29 Aug 2002; NewsScan Daily, 30 August 2002]

<http://www.siliconvalley.com/mld/siliconvalley/news/local/3966648.htm>

✶ **Big Brother hiding inside cars' airbags - tells fibs ([RISKS-22.21](#))**

Bernd Felsche <bernie@innovative.iinet.net.au>

Wed, 28 Aug 2002 11:20:03 +0800 (WST)

Monty Solomon ([RISKS-22.21](#)) drew our attention to the use of recorded information in airbag triggers for crash investigation. Notwithstanding the likelihood that extraction of such measurements doesn't constitute a legal measurement(*), such information extracted must be treated with extreme distrust because the operating environment is not trusted and has many potential modes of unpredictable and unforeseen behaviour.

The recording device isn't measuring road speed at all; rather, it relies not only on its own sensors, but also on information provided by other subsystems in the car. Road speed is most easily (cheaply) obtained by measuring the rate of revolutions of the final drive gearing in the transmission. That speed depends on the speed of rotation of the driving wheels and not the road speed.

One example where the indicated speed is nothing like the true road speed is when one or more drive wheels becomes airborne. Depending on the current driver demand and engine torque, a wide-open-throttle condition results in a very rapid acceleration of the airborne drive wheels, producing a "speed" as high as will be permitted by the engine management system.

How much data are stored is another question. If the recording is only of a second or less of the end to a crash, then it's difficult to establish the sanity of individual data points.

The records may be accurate, but how can you be sure that they reflect what happened in reality?

(*) e.g. http://www.nsc.gov.au/PAGES/Nms/nms_metrology.html

Bernd Felsche - Innovative Reckoning, Perth, Western Australia

✶ FEC OK's SMS spam without saying who paid for it

Hal Murray <hmurray@suespammers.org>

Fri, 30 Aug 2002 12:44:27 -0700

A decision by federal election regulators to exempt text-based wireless ads from campaign disclosure rules has critics warning that consumers could find their mobile phones subject to a flood of political spam as campaign 2002 kicks into high gear.

<http://www.washingtonpost.com/wp-dyn/articles/A49356-2002Aug22.html>

Website Security Flaw Costs ZD

Monty Solomon <monty@roscom.com>

Wed, 28 Aug 2002 23:41:19 -0400

By Brian McWilliams, Wired.com, 28 Aug 2002

Ziff-Davis Media has agreed to revamp its Web site's security and pay affected customers \$500 each after lax security exposed the personal data of thousands of subscribers last year. The settlement, announced on 28 Aug 2002 by New York's Attorney General, could spur other online companies to do a better job securing their sites ...

<http://www.wired.com/news/business/0,1367,54817,00.html>

Transport worker ID in works; privacy rights, funding at issue

Monty Solomon <monty@roscom.com>

Sun, 25 Aug 2002 00:16:26 -0400

The US Transportation Security Administration is developing a mandatory identification card for every trucker, dock worker, airport employee, and mass-transit operator in the nation with access to secure corners of the country's transportation network. ... if implemented, it would be the first broad national identity-card system and could involve hundreds of

thousands of people. [Source: Raphael Lewis, *The Boston Globe*, 24 Aug

2002; PGN-excerpted]

<http://www.boston.com/dailyglobe2/236/nation/>

[Transport worker ID in works+.shtml](#)

✶ The EUR-RVSM safety case is flawed

"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>

Fri, 30 Aug 2002 00:21:16 +0200

Reduced Vertical Separation Minima (RVSM) is a procedure by which the altitude separation between Flight Levels 290 and 410 (that is, between 29,000 ft pressure altitude and 41,000 ft pressure altitude) is reduced to 1,000 ft vertically instead of the previous 2,000 ft vertically. It has been in force in European airspace since early 2002, after trial periods since 1997 on the North Atlantic Track (NAT) and early introduction in Ireland, the UK, Germany and Austria, which was, however, not based on the procedures for the full EUR-RVSM implementation.

However, the argument in the Pre-Implementation Safety Case for RVSM demonstrates at most that RVSM operations without ACAS meet Target Levels of Safety (TLS). It does not demonstrate that RVSM operations with ACAS-equipped aircraft meet Target Levels of Safety; neither can a correct argument for this assertion be reconstructed from the document. The document believes it derives the assertion that RVSM-with-ACAS-meets-TLS from the

assertion that RVSM-without-ACAS-meets-TLS, but the reasoning is flawed and, as far as I can see, irreparable.

Since most aircraft operating in RVSM are required to be ACAS-equipped, the safety case does therefore not establish the required safety level of RVSM operations as they are currently conducted and for the foreseeable future.

The reasoning demonstrating the flaw is contained in the short note "The Pre-Implementation Safety Case for RVSM in European Airspace is Flawed", RVS-Occ-02-03, available from <http://www.rvs.uni-bielefeld.de>

Peter B. Ladkin, University of Bielefeld, <http://www.rvs.uni-bielefeld.de>

✶ Bogus Probabilistic Risk Assessments (Re: Fairfax, [Risks 22.21](#))

"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>
Thu, 29 Aug 2002 04:51:34 +0200

In a note which, inter alia, extols the merits of Probabilistic Risk Assessment (PRA) for assessing risks, Stephen Fairfax claims in [RISKS-22.21](#) that:

Guns in the cockpit represent an independent layer that does not automatically fail when screens fail. While there is heated debate about the possibilities of negative consequences, a dispassionate analysis of the probabilities of both success and failure offers rather

overwhelming

evidence that on balance, armed pilots will reduce both the likelihood and consequences of hijacking attempts.

He claims to be able to assess the probabilities of success and failure (of what, he does not say). I think his assertion is bogus. But it takes advantage of what one might call sound-bite rhetoric. It takes one sentence to assert, but one page to refute, and many people don't have the patience or interest to read that page. Here it is, for those who do.

A PRA works well with physical components. You have a thingummie which is supposed to do thisandthat. You make lots of them, put them on a test apparatus which makes them do thisandthat continuously, and assess a failure rate using well-founded statistical techniques. A physical system has lots of components; lots of different thingummies, so you arrange the failures and their consequences in a taxonomy, plug in the failure rates you have, and do straightforward computations to assess the rates of different kinds of failures of the entire system. This system has worked well for half a century, mainly in the guise of Fault Tree Analysis, and is routine for many applications.

Applying it to components that do not fail that way is rather more tricky. Software, for example. The assessment of SW reliability is a whole branch of statistical methods to itself. It is anything but routine: some very clever people have become famous through their ability to make it sort

of work, sometimes.

Then there is PRA applied to human negotiations. People interacting with each other. Dealing with hijacking is an almost pure negotiation situation. It is not like HW or SW assessment. PRA can be and is performed on negotiation situations, but one requires reliable data, as in the HW case. If you don't have data, whether for hardware, software or wetware, a PRA cannot work. And reliable data for human negotiation situations is very sensitive to environmental variables, many of which one cannot see (it is notoriously difficult to control for cultural dependencies, for example), let alone that infamous variable known to believers in it as free will.

On hijackings in the US, there is no data, none, for the last, oh, thirty years until September 11 last year. The only way that Fairfax could gather data for any of his proposed models would be by simulation, or by patching together data from fragments of behavior inferred from other situations that someone considers relevantly similar.

There is no data, for example, on facility of deployment of a firearm by cockpit crew. That includes the decision to deploy, not just the physical deployment. Second, deployment of a firearm changes the negotiating situation. There is no data on how this negotiating situation will be changed in a commercial airplane. One has to guess: will it be more like a hostage-taking situation, or more like a military firefight amongst civilians? Until September 11, 2001, the assumption was that it

is a hostage situation and pilots were advised accordingly. Opinions have since changed. I emphasise the word "opinions". Those four examples constitute meagre data, as those warning us against "responding by preparing to fight the previous war" have pointed out.

No data, though? Surely El Al's been doing it for years, one might think, and they haven't been hijacked. Exactly: there is no data. No data is not data. One could infer that if one takes over the whole El Al prophylactic package, including the cultural norms and expectations of most of its passengers, maybe one would not have big hijacking problems either, but that proposal is not what is being evaluated. Whatever the El Al example might tell us, it does not tell us anything *probabilistically* about the US domestic consequences of deploying firearms as cockpit equipment, so it's not input to a valid PRA on that issue.

To summarise, I am not aware of any data on which to base a PRA concerning the deployment of firearms in US domestic airline cockpits that is not open to strong objections to its relevance to the situation.

The most worrisome aspect of Fairfax's assertion may be that it is made by a presumed expert in PRA. That is the kind of phenomenon that has led and continues to lead this enormously powerful, essential, but sensitive set of techniques into disrepute. Fairfax is undoubtedly aware that not even the National Academy of Sciences, nor the Royal Society in Britain, recommends

exclusive use of PRA methods as decision procedures for environmental or social policy issues, although they used to until the early 1990's.

Whatever the wisdom or otherwise of deploying firearms on commercial aircraft, the issue should not be determined by arguments with bogus claims to objectivity.

Peter B. Ladkin, University of Bielefeld, <http://www.rvs.uni-bielefeld.de>

⚡ Japanese phones vulnerable to hackers?

Monty Solomon <monty@roscom.com>

Mon, 26 Aug 2002 13:05:48 -0400

Cell phone users in Japan have already had to contend with spam and technical glitches, but that may seem like a breeze when hackers finally turn their attention to the wireless world. So far, no serious virus attacks have been reported in Japan--or anywhere else--but tech security companies say cell phones could become targets as they turn into sophisticated, high-tech devices like PCs, allowing people to send e-mail, surf the Internet and shop online. [...] [Source: Reuters, 26 Aug 2002]

<http://news.com.com/2100-1033-955294.html>

⚡ Microsoft warns of Office and IE risks

"Peter G. Neumann" <neumann@csl.sri.com>

Fri, 23 Aug 2002 11:49:00 PDT

On 22 Aug 2002, Microsoft announced that "critical" security lapses in its Office software and Internet Explorer Web browser put tens of millions of users at risk of having their files read and altered by online attackers.

Using e-mail or a Web page, an attacker could use Internet related parts of Office to run programs, alter data, and wipe out a hard drive, as well as view file and clipboard contents on a user's system. ...

[Reuters, 22 Aug

2002; PGN-ed] <http://news.com.com/2100-1001-954973.html>

✶ Computer expert says he can break Microsoft security

Monty Solomon <monty@roscom.com>

Mon, 26 Aug 2002 19:33:44 -0400

Software security widely used for Internet banking and e-commerce can be easily circumvented, and customer accounts at several of Sweden's largest banks remain at risk as a result, a computer expert said on 26 Aug 2002.

The Swedish hacking expert, who is well known in computer security circles,

but asked not to be named, demonstrated to Reuters how it was possible

within minutes to break through security on Web server SSL software from

Microsoft Corp. He showed how to crack the security systems for Internet

banking, breaking into three of Sweden's big four banks in quick succession.

He was then able to show how to conceal his tracks, making detection

difficult afterward. [Source: Peter Andersson, Reuters, 26 Aug 2002;

PGN-ed] <http://finance.lycos.com/home/news/story.asp?story=28447602>

✂ A better approach to spam

John Pettitt <jpp@cloudview.com>

Tue, 27 Aug 2002 16:20:10 -0700

I'm a former spamcop user. I've switched to a tool called bogofilter

(<http://www.tuxedo.org/~esr/bogofilter/>) which is based on Bayesian

statistics and an article "A Plan for Spam" by Paul Graham

(<http://www.paulgraham.com/spam.html>) the full article presents an

interesting discussion of why keyword filters and block lists don't really

work and suggests a better way based on real math (rather than hunches and suppositions).

For me the statistical approach doing better than spamcop and razor ever

did particularly with respect to false positives.

✂ Re: Keystone SpamCop summary and response (Felten, [RISKS-22.21](#))

Crispin Cowan <crispin@wirex.com>

Wed, 28 Aug 2002 16:38:55 -0700

> ... The ISP was intimidated by SpamCop and seemed to be trying
to show
> that it was responsive to SpamCop complaints. Hence the quick
shutoff of
> my account.

Your ISP did not respond appropriately to Spamcop. They did not
even follow
the directions. The ISP is required to address the issue, not
shut down the
site. Shut down the site is one way of addressing the issue, and
is only
appropriate if actual spamming occurred.

> ... This refusal to reinstate my account is what convinced me
that the ISP
> was afraid of SpamCop.

Sounds like a really bad ISP.

> ... For me, the bottom line is this: if SpamCop didn't exist,
my site
> would not have been shut off.

Near as I can tell from your response, "Blame the ISP, not
SpamCop" still
holds. So change hosting companies; it's not like there's a
shortage of
them.

SpamCop is an immune response to invaders (spam). Like immune
responses, it
can be inconvenient at times. But SpamCop is not nearly so
draconian as you
make out: the draconian effects are all in your ISP's head.

Tell us who the ISP is. They are far more to blame for this than
SpamCop,
and so far they've got off scot-free. Traceroute seems to

indicate it is
"netrail.net" but they do not have a responsive web site.

Crispin Cowan, Ph.D., Chief Scientist, WireX <http://wirex.com/~crispin/>

Security Hardened Linux Distribution: <http://immunix.org>

✦ Parody and copyright (Re: US Navy domain hijacking, [RISKS-22.13](#))

Terry Carroll <carroll@tjc.com>
Sat, 17 Aug 2002 12:15:36 -0700 (PDT)

Jay Ashworth ([RISKS-22.13](#)) reflects a commonly repeated misunderstanding of the Skywalker case, *Campbell v. Acuff-Rose Music*, 510 U.S. 569 (1994), as though it held that parody is not an infringement. The case held no such thing.

The core holding of the opinion is that the lower court had made a mistake by presuming that, because the Campbell parody was a commercial work, its use of the original was presumptively not a fair use and therefore infringing. It then sent the case back down to the lower courts for further consideration in light of the market effect factor.

The Court specifically rejected the argument that parody is inherently a non-infringing fair use. It said that parodies, like any other work, have to be judged on a case by case basis:

Like a book review quoting the copyrighted material

criticized, parody may

or may not be fair use, and petitioner's suggestion that any parodic use

is presumptively fair has no more justification in law or fact than the

equally hopeful claim that any use for news reporting should be presumed

fair, see [Harper & Row Publishers, Inc. v. Nation Enterprises, 471

U.S. 539, 561 (1985)]. The [Copyright] Act has no hint of an evidentiary

preference for parodists over their victims, and no workable presumption

for parody could take account of the fact that parody often shades into

satire when society is lampooned through its creative artifacts, or that a

work may contain both parodic and non parodic elements.

Accordingly,

parody, like any other use, has to work its way through the relevant [fair

use] factors, and be judged case by case, in light of the ends of the

copyright law.

<http://supct.law.cornell.edu/supct/html/92-1292.ZO.html>

Terry Carroll, Santa Clara, CA carroll@tjc.com

✶ Re: American style cyber warfare ... (Hendrik, [R-22.18](#))

Peter Hanecak <hanecak@megaloman.com>

Mon, 29 Jul 2002 09:53:01 +0200 (CEST)

If such law will be passed, I expect RIAA and/or MPPA will start (maybe slowly but definitely) global cyberwar consisting of:

- a) many cracking attacks
- b) many DoS and DDoS attacks
- c) deployment of blocking mechanisms similar to those targeting SPAM ...

and also leading to:

- a) many lawsuits (international too)
- b) demonstrations
- c) trade blockades

and a lot of other consequences - maybe also full scale war (jumping point may be for example computerized war ship - it may answer electronic attack with real rockets - but possibilities are almost endless).



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

[ACM](#) Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 23

Friday 6 September 2002

Contents

- [Appeals court overturns own Web site ruling](#)
[Monty Solomon](#)
- [Citibank e-mailing raises privacy concern](#)
[Monty Solomon](#)
- [Greek government bans electronic games](#)
[Phil Pareas via Max](#)
- [Background checks are more important than education](#)
[Adam Shostack](#)
- [EDIS bulletin on power outages](#)
[Dave Stringer-Calvert](#)
- [Infrastructure risks and Cyberterrorism](#)
[Fred Cohen](#)
- [Re: Homeland Insecurity](#)
[Stephen Fairfax](#)
- [Excellent quote about wireless security](#)
[Al Rizutto](#)
- [Re: Warchalking the Networks](#)
[Michael Cook](#)
- [MS02-050: Certificate validation flaw could enable identity spoofing](#)
[Monty Solomon](#)

 [Info on RISKS \(comp.risks\)](http://comp.risks)

Appeals court overturns own Web site ruling

Monty Solomon <monty@roscom.com>

Wed, 28 Aug 2002 22:24:49 -0400

A lawyer for online privacy-rights group the Electronic Frontier Foundation said a certain amount of inconvenience for police is often the price of protecting privacy. Heeding prosecutors' pleas, the federal appeals court in San Francisco has overturned its own ruling that would have made it much harder to peek at private Web sites.

The unusual reversal by the Ninth U.S. Circuit Court of Appeals came after federal and state prosecutors warned that the ruling would hamper investigations of child molesters who recruit victims online. In its earlier ruling, the court said an airline's furtive entry into a pilot's personal Web site, where criticism of the company was collected, was a possible violation of the federal wiretap law. The 1986 version of that law prohibits any unauthorized interception of an electronic communication.

[Bob Egelko, 28 Aug 2002, <http://www.newsfactor.com/perl/story/19210.html>]

Citibank e-mailing raises privacy concern

Monty Solomon <monty@roscom.com>

Tue, 3 Sep 2002 19:43:58 -0400

In a move that has raised privacy concerns, Citibank used an

outside company
to gather e-mail addresses of its credit-card customers and then
sent
e-mails offering recipients access to sensitive financial data
without
verifying each address actually belonged to the customer.
Citibank is
reviewing the program and said there is a roadblock in place to
prevent
sensitive information from reaching the wrong people. Still, the
matter,
which grew out of a pilot Citibank initiative seeking more
effective
electronic communications with its customers, may raise
questions about
whether federal regulation is needed to ensure consumers' online
privacy is
protected. ... [Source: Messages sent to customers without
address
verification, Yochi J. Dreazen, The Wall Street Journal, 3 Sep
2002]

<http://www.msnbc.com/news/802701.asp>

✶ Greek government bans electronic games

Max <max7531@earthlink.net>
Wed, 04 Sep 2002 17:28:39 -0700

Damn. I didn't believe this message from Phil Pareas at first.
Should be an
interesting test of taking DMCA to the extreme. I just don't
think that
making everyone a criminal is a good way to reduce crime. :) Max

> In Greece, use a Game Boy, go to jail
> By Matt Loney and Rupert Goodwins
> Staff Writers, CNET News.com
> September 3, 2002, 11:18 AM PT

> In Greece, playing a shoot-'em-up video game could land you in jail. The
> Greek government has banned all electronic games across the country,
> including those that run on home computers, on Game Boy-style portable
> consoles, and on mobile phones. Thousands of tourists in Greece are
> unknowingly facing heavy fines or long terms in prison for owning mobile
> phones or portable video games. Greek Law Number 3037, enacted at the end
> of July, explicitly forbids electronic games with "electronic mechanisms
> and software" from public and private places, and people have already been
> fined tens of thousands of dollars for playing or owning games. The law
> applies equally to visitors from abroad: "If you know these things are
> banned, you should not bring them in," said a commercial attaché at the
> Greek Embassy in London, who declined to give her name. Internet cafes
> will be allowed to continue to operate, providing no games-playing takes
> place. If a customer is found to be running any sort of game, including
> online chess, the cafe owner will be fined and the place closed. The
> Greek government introduced the law in an attempt to prevent illegal
> gambling. According to a report in the Greek newspaper Kathimerini, Greek
> police will be responsible for catching offenders, who will face fines of
> 5,000 to 75,000 euros (about \$4,980 to \$74,650) and imprisonment of one to
> 12 months. "The blanket ban was decided in February after the government
> admitted it was incapable of distinguishing innocuous video games from

> illegal gambling machines." ...
> <http://news.com.com/2100-1040-956357.html?tag=dd.ne.dht.nl-hed.0>

✶ Background checks are more important than education

Adam Shostack <adam@homeport.org>

Sun, 1 Sep 2002 18:25:47 -0400

> Thousands of teachers will not be able to take classes at the
> start of the
> new term because character checks on them will not have been
> completed,
> the government has admitted. [...] Leicestershire was one of
> the first
> areas of the country to be affected by the vetting backlog as
> pupils
> returned to school last Thursday, with schools being told to
> turn away
> teachers who had not yet been checked.

http://news.bbc.co.uk/2/hi/uk_news/education/2229196.stm

The mind boggles. Perhaps there's some reason to believe that
Britain's
teachers have suddenly become a particularly questionable lot.
That it is
both worth spending money on checking into their backgrounds and
keeping
them out of classrooms until that's done. That keeping what I'd
guess is
around 140,000 students away from class for a few days is a good
trade off.
Can someone enlighten me as to the particular threat? (Also,
I'm curious
how much the government is spending to keep teachers out of
classrooms?)

(And there are proposals to do this for all 'critical

infrastructure
workers' in the US: "I'm sorry, Mike can't remove the squirrel
from the
transformer until his background check finishes.")

⚡ EDIS bulletin on power outages

Dave Stringer-Calvert <dave_sc@csl.sri.com>

Tue, 03 Sep 2002 16:26:21 -0700

It doesn't take a hacker to shut down the power grid, mother
nature is
quite capable. D_SC

Date: Tue, 3 Sep 2002 16:18:46 -0700

>From: EDIS E-mail Service <edismail@incident.com>

Subject: [EDIS] Law Enforcement Bulletin [Urgent: Statewide]

Emergency services personnel (law enforcement, fire, EMS and
local OES)

throughout Southern California should be advised that the
California

Independent System Operator, the entity that coordinates
statewide flow of

electrical supply, has notified state OES there will be rotating
blackouts

in Southern California with in the next hour due to damage to
major power

lines from fires. [...]

OES Sacramento/Director Dallas Jones/SM

[EDIS is operated by the Governor's Office of Emergency
Services, State of

California. This e-mail relay service is offered by incident.com
on a

non-commercial, subscription-only basis. Because of the
complexity of this

system and its dependence on other systems, we cannot be

responsible for
delays or failures in forwarding or transmission.]

[Upper-case only message lowered to avoid antispam tools. PGN]

✶ Infrastructure risks and Cyberterrorism (Re: Norloff, [RISKS-22.22](#))

Fred Cohen <fc@all.net>

Sun, 1 Sep 2002 21:22:55 -0700 (PDT)

This is a rather complex issue, but one that can be understood in reasonably straight forward terms. At the risk of excessive length, I will proceed as simply as I can...

1) My background: I did some of the initial risk assessments that led to the PCCIP work, some studies as part of the PCCIP study, and some of the subsequent studies - as well as doing work for many of the critical infrastructure providers - some Y2K-related roll-up work on reporting out on these issues, and on and on.

2) A reasonable view: My most reasoned view of the true situation is primarily based on the work related to Y2K in which we considered the potential for all IT failing in the worst possible ways. The goal of much of my effort was to assure that if IT went really bad, national and large-volume human survival would not be impaired. In essence, this has more to do with what happens when it fails than whether it will

fail.

The disaster planning associated with critical infrastructures is, by all that I have seen, ADEQUATE TO PREVENT severe loss of life, serious national security losses, loss of overall military and governmental capability, and unrecoverable economic collapse.

This is not to say that large-scale events cannot happen and that they cannot have large effect. They can. But the severity is not as horrific as many would have others believe. There are some pretty scary scenarios that can be cooked up, and some of them can probably even be made to happen IF WE POSTULATE a large enough and sophisticated enough attacker. But from all I can tell, there is no such attacker, and certainly there are none in the ranks of terrorists I know about or in the ranks of nation states I am aware of - the one exception being the US government itself.

3) SCADA systems in particular: Most SCADA systems are not directly connected to the Internet, and many are not even indirectly connected to it, but this does not mean that there is no risk associated with information attack against these systems. The real questions to ask, however, are not whether some SCADA systems can be defeated and induced to cause serious consequences - they can. The more important question is how complex it would be to coordinate these events across enough of these systems to induce dire consequences that could not be mitigated without severe consequences. This is a much harder thing to accomplish, it takes far more effort, better

intelligence, better coordination, and greater and more focussed resources than typical terrorist groups have - even those with a few hundred million dollars to focus on the effort.

Fred Cohen 1-925-454-0171 <http://all.net/> Sandia Natl Labs 1-925-294-2087

The University of New Haven <http://www.unhca.com/> fc@all.net
[RISKS's default disclaimer specifically invoked here.]

✶ **Homeland Insecurity ([RISKS-22.20](#) to [22](#))**

Stephen Fairfax <fairfax@mtechnology.net>

Sat, 31 Aug 2002 13:18:55 -0400

Peter Ladkin charges that I made "bogus" claims (Homeland Insecurity, Risks [22.20](#), [22.21](#), [22.22](#)) in a classic example of rejecting formal, quantitative analysis because the sparse data make such work messy and inconvenient. I have encountered objections of this nature throughout my career and feel compelled to respond.

The thrust of my comments is that formal thinking and quantitative evaluations appear to be very rare in the introduction of new air transport security measures. Ladkin makes no mention of this point, but seizes on my statement that

"Guns in the cockpit represent an independent layer that does not automatically fail when screens fail. While there is heated debate about the possibilities of negative consequences, a dispassionate

analysis of

the probabilities of both success and failure offers rather overwhelming

evidence that on balance, armed pilots will reduce both the likelihood and

consequences of hijacking attempts."

Without acknowledging the basic logic that adding an additional layer of

defense holds at least the possibility of improving the odds of success,

Ladkin characterizes this statement as "bogus" and "sound-bite rhetoric." (Aside: I used guns in the cockpit because of the current

debate on the issue, but the principle holds true for any defensive

measure. The tone and ad hominem nature of Ladkin's arguments suggest that

I may have offended some deep-rooted beliefs about firearms in general. I

apologize for any inadvertent offense but stand by my argument.)

After a brief explanation of PRA and fault trees, Ladkin goes on to report

that the techniques get much more difficult when applied to software or

human negotiations. I most heartily agree. As one progresses from

hardware to software to "wetware," the complexity of the analysis increases, data grows sparser and more difficult to collect, and the

sensitivity of the results to changes in input data increases.

Ladkin then makes the classic mistake of assuming that a large number of

events without failures constitutes "no data." He writes "On hijackings in

the US, there is no data, none, for the last, oh, thirty years until

September 11 last year." First, even if the implied statement that there

have been no US hijackings in 30 years is true, that does not constitute

"no data." For example, one can ask "Is this record more likely to be attributable to the effectiveness of the present security measures, or does it indicate that the rate of attempted hijacking is very low?" If there had been many attempted hijackings, but they had all been prevented, there would still be no hijackings, but that hardly constitutes a lack of data. Careful study of the records would most likely reveal that there were very few attempts, and one would therefore conclude that it was difficult to assess the efficacy of the current security measures based solely on historic records. (I am generally familiar with aviation safety statistics, but I do not claim to have performed a full study of this issue.) That does not prevent one from doing the assessment in other ways.

Ladkin does not justify excluding data from the rest of the planet. This week's Aviation Week and Space Technology includes a graph from a Boeing Airplane Upset Recovery Training aid that shows 8 fatal accidents, with several hundred fatalities, attributed to hijacking, in the period 1987-96. This hardly constitutes "no data!" Furthermore, as Ladkin surely knows, when data regarding failures is sparse, one searches for "close calls" and other instances where failure was imminent but averted by corrective action or even sheer luck. Indeed, as systems become more and more reliable, failure data gets more and more sparse and therefore more valuable.

Lastly, as Ladkin should know, PRA techniques include methods to

derive

estimates of failure and success probabilities from expert opinion. Experts often have relevant experience with the precursors to failure even if they have not personally experienced the consequences of a failure. Experts also can assist in applying lessons from other fields to the problem at hand. For example, law enforcement and military personnel should be able to produce credible, defensible estimates of the ability of pilots, with some defined level of training, to defend the cockpit, with or without a firearm, from hijackers for a given period of time. The experts need not be commercial airline pilots in order to apply the lessons of one or two defenders against attackers approaching via a narrow corridor. What's more, the estimates derived from expert opinion can be formally compared to historical data, however sparse, to determine the most likely distribution of outcomes. (One point I have ignored for the sake of brevity is that PRA generally deals with probability distributions rather than simple failure rates. Understanding what shapes the distribution is just as important as estimating the magnitude.)

One of the tragedies of September 11 is that there was ample, publicly available data to predict not only the method of attack, but the likely targets. Algerian terrorists hijacked Air France Flight 8969 during the Christmas holidays in 1994. (see <http://www.msnbc.com/news/635213.asp> for a recent summary of those events.) Their plan was to crash a fully fueled airliner into the Eiffel Tower. The plan failed, in large part due to the

courage and resourcefulness of the crew, but also because the terrorists were not trained to fly the aircraft. The terrorists (who may have been associated with Osama Bin Laden) learned from their mistakes; in the US the FAA did not.

There were other warning signs, but I already RISK being PGN'ed. The point is that there was a well documented but unsuccessful attempt by Islamic terrorists to attack a symbolic structure using commercial aircraft as a flying bomb, nearly 7 years before September 11, 2001. Years of inaction by the FAA in the face of a new, very serious threat enabled the success of the later attacks.

Ladkin goes on to demonstrate another pitfall of this admittedly difficult type of analysis. The unchallenged assumption is one of the most dangerous mistakes in any field, as RISKS readers will surely appreciate. Ladkin asserts that "Dealing with hijacking is an almost pure negotiation situation." It was precisely this incorrect assumption that resulted in the FAA mandating that flight crews be trained to cooperate with the terrorists. In an era where well-publicized accounts of suicide bombers successfully attacking civilians appeared on a weekly, sometimes daily basis, the idea that one can negotiate with all hijackers is ludicrous. The unchallenged assumption prevented the people in charge of security from asking obvious "what if" questions that should be an integral part of any high-stakes policy decision.

Ladkin concludes with an assertion that my actions bring the

entire field
of PRA into disrepute, citing scientific societies that no longer endorse
the exclusive use of these techniques in certain areas. A careful reading
of my original comments will show no instance where I suggest that PRA
techniques are the ONLY ones that should be used. On the contrary, I
lament the utter disregard for formal thinking, quantitative analysis, and
public review and discussion of the incredibly expensive measures being
forced on the American public in the name of security. PRA is one of many
tools that could be used to improve this situation, but I would never
suggest that it is the only one, and I reject the charge that I have
somehow sullied the field with my observations.

Issues of security and safety in complex man/machine systems are certainly
difficult to analyze. Controlled Flight Into Terrain (CFIT) continues to
be the number one cause of commercial airline fatalities despite decades of
effort. This problem, like security, involves hardware, software, human
actions and errors, all in a complex, dynamic environment. The fact that
it is difficult to analyze the problem does not obviate the need to do so,
nor does it relieve those who make policies from the responsibility to use
all available tools and techniques in arriving at decisions that literally
mean life and death for thousands. PRA is one such technique, and I stand
by my recommendation that it be used in the analysis of airline security
systems design and operations.

Stephen Fairfax, President, MTechnology, Inc., 2 Central Street
Saxonville, MA 01701 1-508.788.6260 fairfax@mtechnology.net www.
mtechnology.net

[Mispelingz of Ladkin corrected in archive copy. PGN]

✶ Excellent quote about wireless security

<AlRizutto@cs.com>

Wed, 28 Aug 2002 08:38:36 -0400

I found the following line about a wireless security book to be quite interesting:

Writing a book on wireless security is like writing a book on safe skydiving -- if you want the safety and security, just don't do it.

See <http://www.unixreview.com/documents/s=7459/uni1030461766479/>

✶ Re: Warchalking the Networks (Leeson, [RISKS-22.18](#))

Michael Cook <MLCook@aJile.com>

Mon, 29 Jul 2002 10:20:02 -0500

Here's more than you probably want to know about "warchalking" wireless networks. Links to articles are included. Plus, a variety of symbols and their meanings.

<http://www.warchalking.org/>

Michael L. Cook, Technical Staff, aJile Systems, Inc. <http://www.aJile.com/>

MLCook@aJile.com 319-378-3946

★ MS02-050: Certificate validation flaw could enable identity spoofing

Monty Solomon <monty@roscom.com>

Thu, 5 Sep 2002 02:15:29 -0400

Title: Certificate Validation Flaw Could Enable Identity Spoofing (Q328145)
Date: September 04, 2002
Software: Microsoft Windows, Microsoft Office for Mac, Microsoft Internet Explorer for Mac, or Microsoft Outlook Express for Mac
Impact: Identity spoofing.
Max Risk: Critical
Bulletin: MS02-050

Microsoft encourages customers to review the Security Bulletin at:
<http://www.microsoft.com/technet/security/bulletin/MS02-050.asp> .

Issue:

The IETF Profile of the X.509 certificate standard defines several optional fields that can be included in a digital certificate. One of these is the Basic Constraints field, which indicates the maximum allowable length of the certificate's chain and whether the certificate is a Certificate Authority or an end-entity certificate. However, the APIs within CryptoAPI that construct and validate certificate chains (CertGetCertificateChain(),

CertVerifyCertificateChainPolicy(), and WinVerifyTrust()) do not check the Basic Constraints field. The same flaw, unrelated to CryptoAPI, is also present in several Microsoft products for Macintosh.

The vulnerability could enable an attacker who had a valid end-entity certificate to issue a subordinate certificate that, although bogus, would nevertheless pass validation. Because CryptoAPI is used by a wide range of applications, this could enable a variety of identity spoofing attacks. These are discussed in detail in the bulletin FAQ, but could include:

- Setting up a web site that poses as a different web site, and "proving" its identity by establishing an SSL session as the legitimate web site.
- Sending e-mails signed using a digital certificate that purportedly belongs to a different user.
- Spoofing certificate-based authentication systems to gain entry as a highly privileged user.
- Digitally signing malware using an Authenticode certificate that claims to have been issued to a company users might trust.

Mitigating Factors:

Overall:

- The user could always manually check a certificate chain, and might notice in the case of a spoofed chain that there was an unfamiliar intermediate CA.
- Unless the attacker's digital certificate were issued by a CA in the user's trust list, the certificate would generate a warning when validated.

- The attacker could only spoof certificates of the same type as the one he or she possessed. In the case where the attacker attempted an attack using a high-value certificate such as Authenticode certificates, this would necessitate obtaining a legitimate certificate of the same type - which could require the attacker to prove his or her identity or entitlement to the issuing CA.

Web Site Spoofing:

- The vulnerability provides no way for the attacker to cause the user to visit the attacker's web site. The attacker would need to redirect the user to a site under the attacker's control using a method such as DNS poisoning. As discussed in the bulletin FAQ, this is extremely difficult to carry out in practice.
- The vulnerability could not be used to extract information from the user's computer. The vulnerability could only be used by an attacker as a means of convincing a user that he or she has reached a trusted site, in the hope of persuading the user to voluntarily provide sensitive data.

E-mail Signing:

- The "from" address on the spoofed mail would need to match the one specified in the certificate, giving rise to either of two scenarios if a recipient replied to the mail. In the case where the "from" and "reply-to" fields matched, replies would be sent to victim of the attack rather than the attacker. In the case where the fields didn't match, replies would obviously be addressed to someone other than ostensible sender. Either case could be a tip-off that an attack was underway.

Certificate-based Authentication:

- In most cases where certificates are used for user authentication, additional information contained within the

certificate is necessary to complete the authentication. The type and format of such data typically varies with every installation, and as a result significant insider information would likely be required for a successful attack.

Authenticode Spoofing:

- To the best of Microsoft's knowledge, such an attack could not be carried out using any commercial CA's Authenticode certificates. These certificates contain policy information that causes the Basic Constraints field to be correctly evaluated, and none allow end-entity certificates to act as CAs.
- Even if an attack were successfully carried out using an Authenticode certificate that had been issued by a corporate PKI, it wouldn't be possible to avoid warning messages, as trust in Authenticode is brokered on a per-certificate, not per-name, basis.

Risk Rating:

Microsoft Windows platforms:

- Internet systems: Critical
- Intranet systems: Critical
- Client systems: Critical

Microsoft programs for Mac:

- Internet systems: None
- Intranet systems: None
- Client systems: Moderate

Patch Availability:

- A patch is available to fix this vulnerability for Windows NT 4.0, Windows NT 4.0, Terminal Server Edition, Windows XP, and Windows XP 64 bit Edition.

Please read the Security Bulletin at

<http://www.microsoft.com/technet/security/bulletin/ms02-050.asp>

for information on obtaining this patch.

[The information provided in the Microsoft knowledge base is provided "as is" without warranty of any kind. Microsoft disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall Microsoft Corporation or its suppliers be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages, even if Microsoft Corporation or its suppliers have been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of liability for consequential or incidental damages so the foregoing limitation may not apply.] [ALL-CAPS in this paragraph knocked down to avoid antispam tools and annoyed readers. PGN]



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 24

Weds 11 September 2002

Contents

- [Florida Primary 2002: Back to the Future](#)
[Rebecca Mercuri](#)
 - [Nurses refuse to wear locator devices](#)
[Duane Thompson](#)
 - [Computer-Assisted Passenger Screening System defeated](#)
[Max](#)
 - [The Underground Web](#)
[Monty Solomon](#)
 - [Missed phone connections](#)
[Robert Kuttner via Monty Solomon](#)
 - [Microsoft says Win 2000 hacking outbreak subsides](#)
[PGN](#)
 - [Greek court finds Government ban on electronic games unconstitutional](#)
[Giorgos Epitidios](#)
 - [The pinnacle of chutzpah in spam filtering](#)
[Przemek Klosowski](#)
 - [REVIEW: "Computer Forensics and Privacy", Michael A. Caloyannides](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ Florida Primary 2002: Back to the Future

"Rebecca Mercuri" <notable@mindspring.com>

Wed, 11 Sep 2002 03:14:39 -0400

Well, Florida's done it again.

Tuesday's Florida primary election marked its first large-scale roll-out of tens of thousands of brand-new voting machines that were promised to resolve the problems of the 2000 Presidential election. Instead, from the very moment the polls were supposed to open, problems emerged throughout the state, especially in counties that had spent millions of dollars to purchase touchscreen electronic balloting devices.

Florida voters, including Gubernatorial candidate Janet Reno, experienced delays (ranging from minutes to hours) due to touchscreen machines not working properly or at all. Reno, and others (including Duval County officials) reportedly sought court orders requesting additional time for the day's voting session. Governor Jeb Bush granted a two hour extension, but some of the polling places did not receive notice and shut down their machines at 7PM, only to discover that restart was impossible because of the way the machines had been designed.

In addition to polls and machines that opened late, many precincts reported problems with some electronic cards voters used to activate their ballots.

A few machines in Miami-Dade County reset themselves while

voters were trying to vote. Even the mark-sense ballots proved troublesome -- in Orange County many votes will have to be hand-counted because defects made them unreadable by the optical scanners.

Lest readers think that Florida is alone with these election problems, other states, including Georgia and Maryland, have also reported similar difficulties with touchscreens. Problems in MD led 4 counties there to commission a report from UMD, which revealed serious reliability concerns, due to "catastrophic failure," "malfunction," and "unusability" of one of the two machines they were given for testing. The Association of Computing Machinery's Special Interest Group on Computer Human Interaction (ACM SIGCHI) offered to perform similar evaluations on Palm Beach's new voting equipment, urged by U.S. Representative Robert Wexler, but the offer was declined by the County's Board of Elections.

Florida was forewarned about problems with some of their new machines when, in local municipal elections held back in March 2002, anomalies surfaced in Palm Beach County. Some voters submitted sworn affidavits to the state's 15th Circuit Court, attesting to problems ranging from a lack of privacy at the voting booth, to machines "freezing up" until rebooted or reset, and voter cards being rejected.

During this past summer, as part of an investigation into Emil Danciu's contest (one of two lawsuits for the March Palm Beach County election), the

court permitted me to perform a "walk through inspection" of the County's Board of Election warehouse where the machines were being stored and prepared for this Fall's primary. To my amazement, I learned that the devices would not be tested to see whether they would register a vote for each candidate that appeared on the ballot face. Rather, the tallying system was checked by transferring data between cartridges, (circumventing the ballot face on each machine) and only one vote, for the first candidate in each race, was cast using the touchscreen. This essentially meant that most of the new machines would get their first real use only at the actual election. (Not only does this testing lack rigour, but it only marginally complies with Florida election law.)

The Palm Beach County machines were running new software too, since the firmware on each of their 3400 machines was reprogrammed just weeks before the Fall primary. (Such firmware reprogrammability represents a major security and auditability risk.) A thorough inspection of the machines, requested by Danciu's legal team, was denied by the court, on the grounds that the purchase contract with Election Supervisor Teresa LaPore made it a felony violation (for her) of the vendor's trade secret clause if any devices were provided (Danciu had even offered to pay for one) for an internal examination. This trade secrecy also apparently prevents disclosure of the program code files and testing reports maintained by the state of Florida as part of their certification process.

But there's more. Further problems may begin to surface after the tabulation results are analyzed. Although if any candidate wishes to seek a recount, the only one they will get from the touchscreen machines is a printout of the same electronic data residing inside of the machines -- not an independent tally from human-readable ballots that were examined by the voters who cast them on election day. Even Brazil, where 400,000 fully-electronic voting machines were first deployed nation-wide in their 2000 election, deemed it appropriate to retrofit their machines to produce recountable voter-verifiable paper ballots, and they will begin to institute this by modifying some 3% of their machines for their next election.

Sadly, many US communities seem to feel that it is necessary to rush ahead with voting equipment procurements, while reliable systems, appropriate testing, usability, security, and auditability procedures, and other safeguards, are years away. Florida 2000 woke us up to what many already knew -- our voting systems and laws were flawed. Florida 2002 lets us know that expensive computers can not and will not provide the answer to our election troubles.

For the short run, communities that have purchased malfunctioning equipment should return it to the manufacturers and request refunds. There should be an immediate moratorium throughout the United States (and world) on the procurement of electronic voting systems that do not provide voter-verifiable paper ballots. In other words, if your

community is thinking of buying touchscreen or other fully-computerized voting equipment, don't let them do it! Candidates and voters who believe they may have evidence of ballots being lost or foul-play with voting systems, should contact me, as soon as possible, at mercuri@acm.org in order to learn how data could be secured before it may be deleted. Those seeking additional information on voting systems can refer to the numerous articles linked on Peter Neumann's website and on mine (at www.notablessoftware.com/evote.html). Please let your voice and concerns be heard. Democracy is at stake.

Rebecca Mercuri, Ph.D., Bryn Mawr College

*This article is copyrighted property of Rebecca Mercuri (c) 2002.

All rights reserved. Reprint permission is granted only in its entirety, with this notice intact. This article can be distributed but not sold.

For any other uses, please contact the author for permission.*

⚡ Nurses refuse to wear locator devices

Duane Thompson <dst@rmhcn.org>

Fri, 6 Sep 2002 16:31:11 -0700 (PDT)

[This is interesting. It was forwarded via a Healthcare Management e-mail list to which I subscribe. DT]

Since Monday, nearly half of the 120 nurses at Castro Valley, Calif.-based

Eden Medical Center who were assigned to wear personal locator badges as part of a program to provide more efficient care have turned in their devices to protest a system they say invades their privacy and could be misused by managers. The nurse locator system-launched in October on two floors with plans to expand to a third-allows hospital administrators to locate a nurse or a supervisor anywhere at any time. Although the systems, which are used by hospitals across the U.S., can record response times, number of nurse visits to a patient room, and length of time of each visit, Eden uses its \$273,000 system to record only response times. According to hospital officials, the system is meant to help nurses answer patient calls faster and allow the hospital to track nurses more easily in case of emergency. They add that since the installation of the system, patient satisfaction ratings have increased and response times have decreased. But nurses say the devices invade their privacy, interfere with patient care by disrupting conversations between nurses and patients, and contain potentially harmful infrared sensors-a charge the hospital's radiation-safety officer rejects. The nurses note that the hospital has installed the system in the nurses' lounge and kitchen and say that supervisors could use the vocal communication feature to listen in on conversations; the hospital says it has no intention of using the system to listen to nurses. Eden has not taken action against the nurses who refuse to wear the badges. [Reang, *San Jose Mercury News*, 6 Sep 2002; Tate, (Contra Costa Times*, 6 Sep 2002.)]

✈ Computer-Assisted Passenger Screening System defeated

Max <max7531@earthlink.net>

Sat, 07 Sep 2002 11:06:14 -0700

I just read an excellent paper on the inequities of the Computer-Assisted Passenger Screening System (CAPS) for airline travelers (thank you Crypto-Gram), and thought it would add some quantitative analysis to the Homeland Insecurity RISKS debate. Here's the abstract:

To improve the efficiency of airport security screening, the FAA deployed the Computer Assisted Passenger Screening system (CAPS) in 1999. CAPS attempts to identify potential terrorists through the use of profiles so that security personnel can focus the bulk of their attention on high-risk individuals. In this paper, we show that since CAPS uses profiles to select passengers for increased scrutiny, it is actually less secure than systems that employ random searches. In particular, we present an algorithm called Carnival Booth that demonstrates how a terrorist cell can defeat the CAPS system. Using a combination of statistical analysis and computer simulation, we evaluate the efficacy of Carnival Booth and illustrate that CAPS is an ineffective security measure. Based on these findings, we argue that CAPS should not be legally permissible since it does not satisfy court-interpreted exemptions to the Fourth

Amendment. Finally, based both on our analysis of CAPS and historical case studies, we provide policy recommendations on how to improve air security.

And here's a link to the whole paper (the formatting is a little off; scroll down a bit from the title):

<http://swissnet.ai.mit.edu/6805/student-papers/spring02-papers/caps.htm>

✶ The Underground Web

Monty Solomon <monty@roscom.com>

Thu, 29 Aug 2002 04:04:31 -0400

Drugs. Gambling. Terrorism. Child Pornography. How the Internet makes any illegal activity more accessible than ever: It's the kind of call everyone dreads. For Kristen Bonnett, the daughter of NASCAR race driver Neil Bonnett, it came on Feb. 11, 1994--the day her father crashed during a practice run at the Daytona International Speedway. A few hours later, he died. Bonnett was devastated, but she got on with her life. Then, seven years later, came a second call. This time, it was a reporter asking for comment on autopsy photos of her father that were posted on the Internet. Shocked, she quickly got online. "Forty-eight thumbnail pictures, basically of my Dad on the table, butt-naked, gutted like a deer, were staring me directly in the face," says Bonnett. Now, when she thinks of her

father, she
pictures him lying atop an autopsy table.

Warning: You are about to enter the dark side of the Internet.
It's a place
where crime is rampant and every twisted urge can be satisfied.
Thousands
of virtual streets are lined with casinos, porn shops, and drug
dealers. Scam artists and terrorists skulk behind seemingly
lawful Web
sites. And cops wander through once in a while, mostly looking
lost. It's
the Strip in Las Vegas, the Red Light district in Amsterdam, and
New York's
Times Square at its worst, all rolled into one--and all easily
accessible
from your living room couch. ... [*Business Week*, cover
story, 2 Sep 2002]
http://www.businessweek.com/magazine/content/02_35/b3797001.htm

⚡ Missed phone connections

Monty Solomon <monty@roscom.com>
Wed, 28 Aug 2002 23:24:53 -0400

By Robert Kuttner, **The Boston Globe**, 28 Aug 2002

OUR LONG-DISTANCE telephone service stopped functioning
yesterday. For the
magazine I edit, it was a pretty big inconvenience. For several
hours we
pooled cellphones.

My first call was to our bookkeeper. Were we current on our
bills? We were.

My second call was to Qwest, the offending long-distance
company. Its lines

were jammed. A company spokeswoman said she didn't know how many customers had lost service, but Qwest's own filing with the Federal Communications Commission yesterday, as required by law, indicated that 500,000 calls per hour didn't get through. ...

http://www.boston.com/dailyglobe2/240/oped/Missed_phone_connections+.shtml

Microsoft says Win 2000 hacking outbreak subsides

"Peter G. Neumann" <neumann@csl.sri.com>

Tue, 10 Sep 2002 11:19:08 PDT

On 30 Aug, Microsoft warned customers of an increase in reported hacker attacks against Windows 2000, but offered few details about the root of the problem. On 6 Sep 2002, MS said the malicious activity has "lessened significantly" -- claiming that the attacks probably did not result from new vulnerabilities in its operating system, but rather from administrators not following standard procedures to secure their servers. "By analyzing computers that have been compromised, Microsoft has determined that these attacks do not appear to exploit any new product-related security vulnerabilities and do not appear to be viral or worm-like in nature," the company stated in its advisory, available online at <http://support.microsoft.com/default.aspx?scid=kb;en-us;q328691>. "Instead, the attacks seek to take advantage of situations where standard precautions

have not been taken," the advisory said. "The activity appears to be associated with a coordinated series of individual attempts to compromise Windows 2000-based servers." MS urges us to take preventive measures to protect themselves against future attacks: eliminate blank or weak administrator passwords, disable guest accounts, run up-to-date antivirus software, use firewalls to protect internal servers, and stay up to date on all security patches. [Source: article by Matt Berger, *Info World*, 9 Sep 2002; PGN-ed, TNX to Lillie Coney]
<http://www.infoworld.com/articles/hn/xml/02/09/09/020909hnmshack.xml>

[So, it's all OUR fault, even if I don't even use MS software! PGN]

✶ Greek court finds Government ban on electronic games unconstitutional

"Giorgos Epitidios" <gepiti@gepiti.com>
Wed, 11 Sep 2002 15:56:05 +0300

(Re: Pareas via Max, [RISKS-22.23](#))

One of the advantages of Greek law is that every court (no just special ones as in many countries) can decide on the constitutionality of a law. This has its own risks - inconveniences but, I am glad to report that in this case it worked well. The stupid law banning electronic games has been found unconstitutional by the court that was judging the "criminals".

Giorgos Epitidios, Athens, Greece gepiti@gepiti.com

⚡ The pinnacle of chutzpah in spam filtering

Przemek Klosowski <przemek@tux.org>

Wed, 11 Sep 2002 01:24:09 -0400

Recently, I got a piece of spam, which I forwarded to the 'abuse' at the sending ISP (a large, national carrier). I quickly got a reply:

***** Content Filter Notification *****

The following mail was blocked since it contains sensitive content.

Source mailbox: <przemek@tux.org>

Destination mailbox(es): <abuse@....>

Policy: Prohibited Word Filter

I wrote back, without much hope for any effect:

Well, sure the mail contains offending material..

IT WAS SENT TO ME FROM YOU GUYS---THAT'S WHY I AM COMPLAINING

[Why you'd have a content filter on an 'abuse@...' is beyond me.]

[Because they get lots of spam also? PGN]

⚡ REVIEW: "Computer Forensics and Privacy", Michael A. Caloyannides

Rob Slade <rslade@sprint.ca>

Mon, 9 Sep 2002 19:56:41 -0800

BKCMFRPR.RVW 20020604

"Computer Forensics and Privacy", Michael A. Caloyannides, 2001,
1-58053-283-7, U\$79.00

%A Michael A. Caloyannides micky@ieee.org

%C 685 Canton St., Norwood, MA 02062

%D 2001

%G 1-58053-283-7

%I Artech House/Horizon

%O U\$79.00 800-225-9977 fax: 617-769-6334 artech@artech-house.
com

%P 392 p.

%T "Computer Forensics and Privacy"

This book occupies a unique place in the literature of computer forensics. Most works in the field, such as Kruse and Heiser's "Computer Forensics" (cf. BKCMFPRN.RVW), concentrate on documentation of the investigation with a view to presentation in court. The actual mechanics of data recovery tend to be left to commercial tools. Caloyannides demonstrates how to delve into corners of the computer in order to actually get the data out.

At the same time, this work is inconsistent, on at least two levels.

The perspective flips back and forth between forensics and privacy, alternately emphasizing how to find evidence, and how to hide evidence. The technology involved is the same, but the shifts in viewpoint can be jarring to the reader. At the same time, the depth of technical detail can vary wildly. At one point the book stops shy of telling you how to undelete files with a sector editor (an activity that could be useful to every computer user), while other sections

list lengthy and extraordinary measures to secure personal computers.

Part one concentrates on the data recovery aspect of computer forensics. Chapter one is entitled an introduction, but seems to be more of an editorial on privacy, with the added statement that the book is intended both for law enforcement personnel needing details of computer forensic techniques and those wishing to preserve the privacy of data. The use of, and factors related to the use of, computer forensics is supported by specific cases (rather than vague suppositions) in chapter two. One has to agree with the author's statement, in chapter three, that "computer forensics can be done-- and, sadly, is often done--by persons with a minimal amount of either education or experience." Therefore it is unfortunate that the forensic tools list and book structure are both difficult at this point, although there is good material and writing, and Caloyannides is not afraid to tackle the social and political aspects of the field. Chapter four outlines various places (primarily in Windows) from which data may be recovered. It is an odd mix of little known and very valuable information, and extremely poor explanations of basic functions like manual undeletion and file overwriting. A strange and terse look at steganography, US and UK surveillance systems, cryptography, and anonymity makes up chapter five. Data acquisition, from sources such as key logging and Van Eck radiation, is reviewed in chapter six. Chapter seven debunks a short list of measures falsely believed to provide privacy protection.

Part two turns to privacy and security. Chapter eight is a discussion of legal and commercial protections of privacy (mostly in the

US) and their failings. Installing and configuring a privacy protected configuration of Windows is covered in chapter nine, in considerable detail. Chapter ten's review of basic online privacy is heavy on additional software packages. Intermediate online privacy, in chapter eleven, looks at browser and email configurations, more packages, and has a section on tracing email that would be helpful in dealing with spam. (An unfortunate typesetting error seems to have deleted what might have been valuable information about PGP [Pretty Good Privacy].) Chapter twelve is more advanced, dealing with anonymizing services and personal firewalls, but may be beyond the average user. A general opinion piece on cryptography, chapter thirteen nevertheless provides a good, basic background, albeit with a social and political emphasis. Chapter fourteen looks at more practical encryption, detailing PGP and specialized cryptographic programs, with a detour into biometrics.

Part three is a brief look at legal and other issues. Chapter fifteen is a brief look at laws, mostly in the US. Chapter sixteen touches on security aspects of VoIP (Voice over Internet Protocol) and GSM (Global System for Mobility) wireless services.

Despite the ragged organization and style, and some glaring gaps in coverage, this book does contain a wealth of information for both the computer forensic examiner, and the user concerned with privacy. For anyone beyond the most basic user it is well worth a read.

copyright Robert M. Slade, 2002 BKCMFRPR.RVW 20020604
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

<http://victoria.tc.ca/techrev> or <http://sun.soci.niu.edu/~rslade>



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

[ACM](#) Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 25

Monday 23 September 2002

Contents

- [Elections In America - Assume Crooks Are In Control](#)
[Lynn Landes via Rebecca Mercuri](#)
- [Re: Florida Primary 2002: Back to the Future](#)
[Bob Morrell](#)
- [Georgia Secretary of State response to Mercuri](#)
[Chris Riggall via Donald R. Calabro Jr.](#)
- [Election idiocy crosses state lines](#)
[Mark Richards](#)
- [Retrospective Karger/Schell paper on Multics Security Evaluation](#)
[Steve Summit](#)
- [Info on RISKS \(comp.risks\)](#)

✶ Elections In America - Assume Crooks Are In Control, Lynn Landes

"Rebecca Mercuri" <notable@mindspring.com>
Wed, 18 Sep 2002 09:09:35 -0400

[Spin Doctors at it again! Rebecca.]

Elections In America - Assume Crooks Are In Control

Lynn Landes, 16 Sep 2002

Don't blame the poll workers in Florida. The facts, supported by voting machine experts and numerous newspaper articles, have made it clear. Computerized voting machines that were certified by the state of Florida, caused most of the problems in Florida's primary election. In the absence of paper ballots, the damage is now irreversible.

This was no accident. It's not new. And Florida is not alone.

"The concept is clear, simple, and it works. Computerized voting gives the power of selection, without fear of discovery, to whomever controls the computer," wrote the authors of *VoteScam* (1992), James & Kenneth Collier (both now deceased). It's a 'must read' book about how elections have been electronically and mechanically rigged in the United States for decades, and with the knowing and sometimes unknowing support of media giants and government officials, including... ironically... Janet Reno.

Only a few companies dominate the market for computer voting machines.

Alarmingly, under U.S. federal law, no background checks are required on these companies or their employees. Felons and foreigners can, and do, own computer voting machine companies. Voting machine companies demand that clients sign 'proprietary' contracts to protect their trade secrets, which prohibits a thorough inspection of voting machines by outsiders. And, unbelievably, it appears that most election officials don't

require paper ballots to back up or audit electronic election results. So far, lawsuits to allow complete access to inspect voting machines, or to require paper ballots so that recounts are possible...have failed.

As far as we know, some guy from Russia could be controlling the outcome of computerized elections in the United States.

In fact, Vikant Corp., a Chicago-area company owned by Alex Kantarovich, formerly of Minsk, Belorussia (also known as White Russia, formerly U.S.S.R.), supplies the all-important 'control cards' to Election Systems & Software (ES&S), the world's largest election management company, writes reporter Christopher Bollyn. According to ES&S, they have "handled more than 40,000 of the world's most important events and elections. ES&S systems have counted approximately 60% of the U.S. national vote for the past four presidential elections. In the U.S. 2000 general election, ES&S systems counted over 100 million ballots."

Getting back to Kantarovich, he would not disclose where the control cards are made, except they aren't made in America, writes Bollyn. Nor would he discuss his previous employment. Bollyn says he got some not-too-thinly-veiled threats from Kantarovich.

Kantarovich sounds more like the Russian mafia, than a legitimate businessman.

But the really big deal is this....all of ES&S's touch screen machines contain modems, "allowing them to communicate-and be communicated with-while

they are in operation," reports Bollyn. That communication capability includes satellites. "Even computers not connected to modems or an electronic network can still be manipulated offsite, not during the election, but certainly before or after," says voting systems expert Dr. Rebecca Mercuri.

ES&S supplied the touch screens for Miami-Dade and Broward counties where the worst machine failures occurred. But the debacle was nothing new for ES&S. Associated Press (AP) reporter Jessica Fargen wrote in June 2000, "Venezuela's president and the head of the nation's election board accused ES&S of trying to destabilize the country's electoral process. In the United States, four states have reported problems with equipment supplied by the company. Faulty ES&S machines used in Hawaii's 1998 elections forced that state's first-ever recount."

Sequoia is another voting systems company that sends a cold chill down my spine. "Mob ties, bribery, felony convictions, and threats of coercion are visible in the public record of the election services company," according to investigative journalist and filmmaker Daniel Hopsicker, and reported in Spotlight.com. Hopsicker says that Pasquale "Rocco" Ricci, a 65-year-old senior executive with Sequoia, and the firm's Louisiana representative, recently pled guilty to passing out as much as \$10 million dollars in bribes over the course of almost an entire decade." According to American Law Education Rights & Taxation (ALERT), Ricci is the president of

Sequoia

International, which also manufactures casino slot machines.

That's just great. Now, we could possibly have both the Russian mafia and the U.S. mafia involved in our elections.

In May 2002 Sequoia was bought by De La Rue, based in England. By their own estimate, De La Rue is "the world's largest commercial security printer and papermaker, involved in the production of over 150 national currencies and a wide range of security documents such as travelers checks and vouchers. Employing almost 7,000 people across 31 countries, (De La Rue) is also a leading provider of cash handling equipment and software solutions to banks and retailers worldwide." And they develop technology for secure passports, identity cards, and driver's licenses.

Okay, add Dr. Evil to the mix and be on the look-out for international money launderers, drug kingpins, and Nazis.

The Shoup Voting Solutions of Quakertown, Pennsylvania, has a reputation for rigging elections, wrote the late co-author of VoteScam, Jim Collier. According to Collier, in 1979, Ransom Shoup II, the president of the firm, was convicted of conspiracy and obstruction of justice stemming from an FBI investigation of a vote-fixing scam involving the old-fashioned lever machines in Philadelphia."

These reports are just the tip of the iceberg. The numerous instances of U.S. voting systems error and fraud are documented in a 1988 report for the U.S. Commerce Department entitled, "Accuracy, Integrity, and

Security in
Computerized Vote-Tallying" by Roy G. Saltman, a computer
consultant for the
National Institute of Standards and Technology's Computer Systems
Laboratory. Many other experts and observers have been warning
and
complaining about these problems for decades.

But complaints, warnings, reports, and books like "VoteScam,"
haven't
deterred government officials like Pinellas County (Florida)
Commissioners
Calvin Harris and County Judge Patrick Caddell. They told the
St. Petersburg
Times in October 2001 that they were aware that all of the
voting machine
companies had "problems in their pasts." But, Harris said, "We
have to look
at this objectively and not get tied up into the emotions of,
'Some guy
might be a crook."

Dear Commissioner Harris...when it comes to elections in
America...assume
crooks are in control...and then act accordingly.

Links:

- a.. <http://www.votescam.com>
- b.. <http://www.securepoll.com>
- c.. <http://www.commondreams.org/views02/0805-07.htm>

Lynn Landes, 217 S. Jessup Street, Philadelphia, PA 19107 /
(215) 629-3553 /
(215) 629-1446 (FAX & ISDN) lynnlandes@earthlink.net
Lynn Landes is a freelance journalist specializing in
environmental issues. She
writes a weekly column which is published on her website [www.
EcoTalk.org](http://www.EcoTalk.org) and
reports environmental news for DUTV in Philadelphia, PA. Lynn's
been a radio
show host and a regular commentator for a BBC radio program.

✦ **Re: Florida Primary 2002: Back to the Future (Mercuri, [RISKS-22.24](#))**

"Bob Morrell" <bmorrell@wfubmc.edu>

Wed, 11 Sep 2002 13:18:09 -0400

I think the problems with the Florida voting system could be used as a case study on how not to implement a computerized system. Indeed, any intelligent analysis of the tasks and resources should have warned designers that significant problems were ahead. Device use is infrequent. The staff responsible for the devices (poll watchers) are usually undertrained volunteers, often elderly retirees with little experience with electronic devices, much less computers. Overall system management responsibility is completely decentrallized and has low priority in all locations. The main user (voters) are completely untrained. The frequency of exceptions to rules and the need for override capability is high (flying in the face of the needs for security) and resource allocation (after the initial post 2000 flurry of concern) for changes and needed alterations is extremely low. Some of the problems listed by Rebecca Mercuri ([Risks Digest 22.24](#)) and in the general media are so incredible, one has to assume that the vendor selected for the contract won bid by cutting some very basic corners.

I think that Mercuri's call for a moratorium throughout the United States

(and world) on the procurement of electronic voting systems that do not provide voter-verifiable paper ballots is the starting point for reform. But beyond that, given the current operational parameters, one has to ask whether this system, as is, can be computerized to any great degree.

Bob Morrell <http://home.triad.rr.com/bmorrell/>

★ Georgia Secretary of State response to Mercuri in [RISKS-22.24](#)

"Donald R. Calabro Jr." <Don@Calabro.com>

Mon, 16 Sep 2002 20:29:17 -0400

This is a response to Rebecca Mercuri's article "Florida Primary 2002: Back to the Future," from Chris Riggall, The Press Secretary for Cathy Cox, GA Secretary of State.

Mr. Calabro: Thanks for your message, and for passing along the response from Ms. Mercuri.

I'm not sure what issues Ms. Mercuri refers to as far as the equipment in Georgia is concerned, but I'll try to take a stab at it. We operated the new AccuVote TS systems in two counties in the Aug. 20th Primary and Sept. 10th runoff elections. The performance of the equipment in these "real world" settings was quite good, and based on both media accounts and our personal visits to precincts those days in Hall and Marion Counties, the response of

voters was overwhelmingly positive.

On the Primary Aug. 20th, many of the other 157 counties also had the equipment displayed in voting precincts with a demonstration ballot. This was one component of a broad based voter education campaign -- to let voters see for themselves the new technology they would vote on in November. Among these units about five percent reported problems with screen freezes -- and the solution in that circumstance is to turn the unit off, then back on again. This was unfortunate, but not unanticipated since several weeks prior to the primary Diebold and we became aware that this problem could occur and was the result of a conflict between the unit's firmware and a new release of Windows CE that serves as the units' operating system (as a PR guy, I'm on shaky ground trying to explain this to an IT expert!). Diebold programmers developed a patch which was applied to the units deployed in Hall and Marion counties, and we were pleased that not one freeze was reported among the tens of thousands of votes cast there. Unfortunately, we simply did not have the time to apply the patch to the demo units, but that is now occurring to all units in all counties and the last increment of shipments from Diebold had this fix loaded before leaving the factory.

Not referring to Ms. Mercuri, of course, but we have had some wild allegations about equipment failures in Hall and Marion during these two elections. One Georgia political party chairman (he'll go unnamed) put out

a news release claiming that voters in one Hall precinct were turned away because of equipment failures and were issued "vouchers" so they could return and vote later. Balderdash. Never happened.

Regarding Maryland, the coverage that I saw of that election using Diebold equipment last week came from the Washington Post -- not exactly an uncritical media outlet. The primary complaints from that seemed to be focused on Montgomery County, (one of four counties using that equipment -- representing 40 % of that state's voters) where results were relatively slow to be compiled and reported. While slow reporting is not ideal, it is not in the least the kind of critical failure that occurred in two Florida counties (Dade and Broward) out of the 15 that deployed new DRE systems last Tuesday.

We would completely agree, and media accounts from Florida suggest, that the critical issue is education of voters and, even more importantly, poll workers before the election takes place. We are putting a tremendous focus on this and providing to the counties an array of training and technical support -- including hands-on classroom training for about 6,000 poll workers. I think her suggestion about using college IT students is an excellent one, and we have been working with county election officials for a year to help them expand their poll worker recruitment efforts and expand their traditional pool to include teachers, students and others with some level of technical knowledge.

Also regarding Maryland, I thought I would include some information Diebold put out last week -- don't mean to burden you with corporate PR stuff, but there are some quotes from Maryland election officials which I thought you would find of interest.

Again, thanks for contacting us. I know that not every single thing on Nov. 5th will take place perfectly (no election has ever met that standard) but we are very cognizant of the training issues and are working hard to make sure the counties perform in this critical area. Here's the Diebold info:

DIEBOLD TOUCH-SCREEN VOTING TERMINALS PERFORM WELL IN PRIMARY ELECTIONS

Voters in Maryland, Georgia and Kansas Show Widespread Acceptance to New Technology

Photo available at <http://www2.diebold.com/whatsnews/pr/photo.htm>

NORTH CANTON, Ohio - Diebold Election Systems, Inc., a wholly owned subsidiary of Diebold, Incorporated, today announced its touch-screen voting terminals performed extremely well in four counties within the state of Maryland. This election marks the state's first widespread use of the new AccuVote-TS electronic touch-screen voting system to be deployed statewide for future elections.

Over 40 percent of the state's 2.7 million registered voters, located in four counties -Montgomery, Prince George's, Allegheny, and Dorchester - were

the first to use the new electronic voting system in Tuesday's primary election.

Currently, Diebold has touch-screen voting systems in more than 170 counties in many states throughout the United States, totaling more than 35,000 voting stations. Diebold's touch-screen system was not utilized in the recent Florida primary election.

"The response from voters was absolutely positive," said Margaret Jurgensen, election director, Montgomery County Board of Elections. "I spoke to many voters after they cast their ballots, and they stated that they loved the ease of voting with the new system. Many voters commented about the ease of reading the ballot on the touch screen. One visually impaired voter was able to vote for the first time without assistance because of the ballot magnification feature of the system. As with any new technology, our election staff grew more comfortable with the system as the day progressed, and we see the implementation of the touch screen system continuing to improve as our staff becomes more familiar with the technology."

"Our first touch screen primary election was a tremendous success," stated Donna Rahe, Dorchester County election director. "The voters of Dorchester County adapted to the touch screen technology extremely well, and the combined coordination efforts of the county's election staff and Diebold Election Systems caused a very smooth transition to the new election system."

Diebold experienced similar success in August when voters in Hall and Marion counties in the state of Georgia tallied primary election results on the touch-screen voting system. Georgia is the first state in the country to implement a uniform statewide, computerized touch-screen voting system. Earlier this year, Diebold announced a \$54 million agreement with Georgia officials to overhaul the state's election system technology making the state a national leader in replacing outdated election equipment.

"Georgia's new uniform electronic voting system received its first test in the Primary Election and the Diebold units passed with flying colors," said Georgia Secretary of State Cathy Cox, Georgia's chief elections official.

"Throughout Hall and Marion Counties we heard extremely positive comments from voters and poll workers about the convenience, security and ease of use of the new AccuVote-TS units."

Voters in Johnson County, Kansas, were pleased with the touch-screen system as well. Approximately 99-percent of the voters who completed a comment card after using the system gave it a favorable rating.

"The Johnson County Election Office is proud of its reputation of making voting convenient and accessible," said Connie Schmidt, Johnson County Election Commissioner. "We are pleased to be the first county in the Midwest to deploy touch-screen voting computers to all polling places countywide."

"Considering the magnitude of these elections, which includes more than 870,000 registered voters within the four Maryland counties, we are very pleased with the results as every single vote was accurately counted," said Bob Urosevich, president of Diebold Election Systems, Inc. "Increased familiarity with the system will continue to make the process even smoother in future elections. We are working with the voters, poll workers and election officials to ensure that the entire process is intuitive and streamlined for everyone involved."

Chris Riggall
Press Secretary
Ga. Secretary of State Cathy Cox
110 State Capitol Atlanta, Ga. 30334
404-656-5792

✶ Election idiocy crosses state lines

"Mark Richards" <mark.richards@massmicro.com>
Thu, 19 Sep 2002 16:31:22 -0400

When America sends its youth to war, at least in the past, it was for protecting our freedoms. Now we send our youth to war on the whim of a weak mind, one incapable of uttering a coherent English sentence, drawling nonsense rhetoric. What for? Oil of course. But that's not important right now.

What's really important is that the sort of thing people died for in wars past, the right to a fair and free election, is in the hands of

those with
little or no mind power, so well-proven by the recent Florida
mess, defa vu
all over again. I haven't read a single commentator who stood
up and
suggested that the whole thing is downright unpatriotic; a stain
on the
graves of those who died.

Election people, even when given lots of money and another
chance,
managed to screw up, royally. We can certainly blame the
computers and
the complexity and moan about the lack of testing, redundancy and
safeguards. But when I read the news from Marlboro,
Massachusetts, and
the fact that, for the second year, the election people screwed
up
again, it makes me wonder if The Florida Disease, like the West
Nile
virus, is spreading northward.

According to the *Metrowest Daily News*, a snafu brought their
vote-tabulation system to its knees and resulted in the
necessity to
hand-count the ballots. I always appreciate it when the press or
officialdom bring out these cute terms like snafu and glitch.
Makes these
blunders seem, well, harmless.

Last year's problem? The people maintaining the city's computer
system
didn't know last year why the clerk's office was on the computer
system
after hours and kicked it off while doing its nightly backup
work.

This year? No one seems to know. This year, however, the
systems
administrators didn't try to back up the files being used by the
clerk's
office, Bunting said, so she doesn't know what happened.

But don't worry. Next year (the third time) will be a charm. We are comforted to hear, The problem shouldn't affect a third election, Bunting said. She said she's in the final stages of moving City Hall offices off of a 20-year-old computer system and onto a personal computer system.

Massachusetts just suffered one of the worst voter turn outs in record. Idiot blunders like these do little to raise confidence that one vote counts.

Retrospective Karger/Schell paper on Multics Security Evaluation

Steve Summit <scs@eskimo.com>
Thu, 12 Sep 2002 11:00:06 -0400

I'm sure that many, many readers of RISKS are familiar with the story of Ken Thompson's Turing Award lecture: of the invisible trapdoor in /bin/login maintained by an equally invisible trapdoor in the compiler, of the oblique reference to an "unknown Air Force document" whence came the idea for the trapdoors, of Ken's request for anyone who knew of the actual paper to let him know. What I, for one, did not know was that the paper and its authors had in fact come to light: "Multics Security Evaluation: Vulnerability Analysis", written by Paul A. Karger and Roger R. Schell and published by the Air Force in 1974. And in a new paper which is

simultaneously a trip
down memory lane and an up-to-the-moment call to arms, Karger
and Schell
have collaborated on a new, retrospective paper which reviews
(and
incorporates a resurrected copy of!) the former report, while
analyzing
today's computer security landscape in light of the former
report's analyses
and recommendations.

The new paper is "Thirty Years Later: Lessons from the Multics
Security
Evaluation". It is to be presented at the Annual Computer
Security
Applications Conference (ACSAC, <http://www.acsac.org/>) in
December, and a
preprint copy is available under <[http://domino.watson.ibm.com/
library/
cyberdig.nsf/papers?SearchView&Query=\(multics\)](http://domino.watson.ibm.com/library/cyberdig.nsf/papers?SearchView&Query=(multics))>. Anyone
remotely interested
in computer security (which probably includes just about
everyone reading
RISKS) should probably not bother reading any more of this note
of mine, but
should head directly to the domino Web site to fetch a copy.
It's an
excellent read, and the opportunity to view the problem from the
1974
perspective -- via the incorporated copy of the 1974 paper -- is
priceless.
(Among other things, it makes you realize how little we've
learned since.)

Dismayingly, but not surprisingly, the authors do not find that
the
operating systems of today have benefited much from their in-
depth analyses
of Multics. Multics with moderate improvements was, they felt,
adequately
secure for a closed environment, but would not have been secure
in an open
environment (i.e. accessible to untrusted users) without a new

security

kernel which was never completed. Today's popular operating systems, on the other hand, are barely as secure as the unimproved Multics was, yet of course they are routinely asked to serve in the very harshest of environments: the open Internet.

I'm afraid that the paper may be dismissed by some as another antiquarian

pro-Multics rant, and I've also seen suggestions that it's thinly disguised

Microsoft- or Unix-bashing. Neither criticism is remotely accurate: the

paper's analysis is impartially objective and if anything borders on the

excessively sober. To point out security flaws in popular operating systems

is not to bash them; those problems are simple facts.

My only criticism of the paper is not a criticism but a lament, similar to

the one I sometimes feel when reading RISKS these days. Those of us who

like to think we understand security have been discussing these issues for

decades, but the message does not seem to be getting out; systems at all

levels remain variously depressingly or laughably insecure. The current

activity surrounding security is almost all what Karger and Schell call a

"battle of wits" between attackers and defenders; little is being done to

make commodity systems fundamentally secure.

The obvious concluding question -- of a paper like Karger and Schell's, or a

review like this one -- is, what should be done? The authors are not

dogmatic, merely pointing out that the current situation is unstable and

that some truly secure mechanisms (already known to be both

theoretically
and practically viable) will have to be deployed lest chaotic
disasters
ensue. The question for the rest of us is, do we agree, and can
we persuade
the parties who matter that they've got to take security more
seriously? An
all too likely reaction to the paper is that its insistence on
new,
verifiably secure kernels is extreme and unnecessary, that all
we've got to
do to win the "battle of wits" is to try a little harder. Alas,
it's not
clear that we're even keeping up with the adolescents who
perpetrate
scourges like Nimda and Klez, and it's even more unpleasant to
contemplate
how we might fare if faced with "industrial-strength
espionage" (as Vernor
Vinge put it in his haunting novel *Marooned in Realtime*). Let's
hope we can
find the collective wherewithal to do **something**; I'd rather
not find
myself marooned in the postapocalyptic husk of a once-great but
inadequately
secure cyberspace.

Steve Summit <scs@eskimo.com>

[The Web version has an explicit caveat relating to the fact
that the
two papers have been submitted to the Classic Papers section
of the 18th
Annual Computer Security Applications Conference (ACSAC), 9-13
Dec 2002,
Las Vegas NV, and that until then the papers are considered
restricted
in their distribution. However, discussion of these papers
has already
reached Slashdot. We include this notice here to encourage
discussion
of their RISKS-relevance, and to encourage your attendance at
ACSAC if

this topic interests you, not to induce you to violate the
caveat on the
watson.ibm.com site. PGN]



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 26

Weds 25 September 2002

Contents

- [Press Releases MIT vs Mercuri](#)
[Rebecca Mercuri](#)
- [Cost cutting endangers hospital power](#)
[Rich Brown](#)
- [South Wales train leaves without driver](#)
[Fuzzy Gorilla](#)
- [Greek government doesn't quite ban electronic games](#)
[Bruce Anderson](#)
- [Yet another intrusive Web site](#)
[Michael Ortega-Binderberger](#)
- [Air passenger jailed for using mobile](#)
[George Roussos](#)
- [Re: Microsoft says Win 2000 hacking outbreak subsides](#)
[Mike Patnode](#)
- [Re: The pinnacle of chutzpah in spam filtering](#)
[Peter Corlett](#)
- [Re: Retrospective Karger/Schell paper on Multics Security Evaluation](#)
[Paul Karger](#)
- [REVIEW: "Pearl Harbor Dot Com", Winn Schwartau](#)
[Rob Slade](#)

 [Info on RISKS \(comp.risks\)](#)

Press Releases MIT vs Mercuri

"Rebecca Mercuri" <notable@mindspring.com>

Tue, 24 Sep 2002 13:44:34 -0400

I was forwarded the following press release from MIT/CalTech from a source at IEEE Spectrum and am seriously concerned about the conclusions they have drawn regarding the recent Florida primary election. The press release is here in its entirety, followed by my analysis/rebuttal. R. Mercuri.

>Date: Thu, 19 Sep 2002 10:56:22 -0700

>To: Recipient List Suppressed;;

>Subject: Caltech-MIT Team Find 35% Improvement in Florida's Voting Technology

>For Immediate Release

>September 19, 2002

>Caltech-MIT Team Finds 35% Improvement in Florida's Voting Technology

>PASADENA, Calif. - If one measures election success by equipment performance alone, Florida's push to get new voting equipment on-line for the 2002 election appears to have paid off.

>Compared with the performance of equipment in past Florida state primary elections, the new technologies for casting and counting ballots look like clear improvements according to experts at the California Institute of Technology and the Massachusetts Institute of Technology.

>Researchers from the Caltech/MIT Voting Technology Project

>calculated the rate of residual votes (ballots on which no
 votes or
 >too many votes were recorded) for the largest counties in
 Florida
 >for the 2002 Democratic Gubernatorial Primary and for the last
 three
 >Gubernatorial General Elections in Florida (1990, 1994, and
 1998).
 >These counties are Brevard, Broward, Duval, Hillsborough,
 >Miami-Dade, Palm Beach, and Pinellas.

>The residual vote rate, it appears, has been substantially
 reduced
 >as a result of the election reform efforts of the past year. On
 >average, 2.0 percent of Democratic voters recorded no vote for
 >governor in these seven counties. In past elections, the
 average
 >has been 3.1 percent. This is a 35 percent improvement in
 >performance.

>The largest apparent improvements came in Brevard and Duval
 >counties, which switched from punch cards to optically scanned
 paper
 >ballots. The remaining counties purchased new touch screen or
 >Direct Recording Electronic (DRE) machines. All of the counties
 >show some improvement in their capacity to record and count
 votes.

>Residual Vote Rates for Governor in the 7 Largest Florida
 Counties

>County	2002	1998	Ave.	1998	1994	1990
>Brevard	1.0% Scanner	Punch	4.2%	2.6%	4.5%	5.4%
>Broward	2.0 DRE	Punch	2.6%	2.7	1.9	3.3
>Dade	3.0 DRE	Punch	3.2%	4.0	2.7	3.2
>Duval	2.2 Scanner	Punch	3.4%	3.1	2.5	4.5
>Hillsborough	1.6 DRE	Punch	2.3%	2.7	1.9	N/A
>Palm Beach	2.3 DRE	Punch	3.1%	3.7	2.3	3.3
>Pinellas	1.9 DRE	Punch	2.2%	2.3	1.9	2.3
>Total	2.0		3.1%			

[General elections; PGN approximate reconstitution of a
 garbled table]

>Source: Florida Division of Elections and county election
offices
>of each county.

>(This table may lose formatting in your email program, see
accurate [...])

>"These results are very encouraging," said Stephen
Ansolabehere, a
>professor at the Massachusetts Institute of Technology and
>co-director of the project. "Florida made a major effort to
upgrade
>its technology and, in the primary, the machines used showed
clear
>gains over the technologies in past elections."

>Professor Charles Stewart, another MIT professor working on the
>Voting Technology Project, cautions that "the success of an
election
>cannot be measured solely in terms of equipment performance.
>Current events in Florida also illustrate how better technology
is
>just a first step in improving the functioning of democracy."
>Stewart said, "Most of the problems reported by journalists
covering
>the 2002 Primary Elections in Florida did not concern equipment
>malfunctions, but problems encountered preparing for election
day,
>such as training poll workers."

>R. Michael Alvarez, co-director of the Voting Technology
Project and
>professor of political science at the California Institute of
>Technology, said "As counties and states across the country,
>especially here in California, plan out similar changes, we are
>learning important lessons about how to make such important
changes
>in voting technologies."

>"The one distressing thing, though, are the reports from Florida
>that polling place workers had difficulties getting some of the
new

>voting machines up and running on election day in Florida, and
>that
>as a result, some voters might have been turned away from the
>polling places. These reports reinforce our calls for more
>polling
>place workers and better training of polling place workers, as
>they
>provide a critical role in making sure that all votes are
>counted,"
>Alvarez said.

>MIT's Stewart adds "The fact that the congressional election
>reform
>bill is currently stalled in a House-Senate conference committee
>hasn't helped matters any."

>The Caltech/MIT Voting Technology Project is a non-partisan
>research
>project, formed to study election systems following the 2000
>presidential election and sponsored by the Carnegie Corporation.
>More information and copies of reports are available at
>www.vote.caltech.edu.

>MEDIA CONTACT: Jill Perry, Caltech Media Relations Director
> (626) 395-3226

> Sarah Wright or Ken Campbell, MIT News Office
> 617 253-2700

>Jill Perry
>Media Relations Director
>California Institute of Technology (Caltech)
>Mailing Address: Mail Code 0-71, Pasadena, CA 91125
>Street Address: 315 S. Hill Ave., Pasadena, CA 91106
>Ph: (626) 395-3226
>Fax: (626) 577-5492
>jperry@caltech.edu

- - - - -

NEWS RELEASE, September 24, 2002

Rebecca Mercuri rebuts recent MIT/CalTech voting systems

analysis and
calls for moratorium on new electronic balloting equipment
purchases

After reviewing the press release issued September 19 by MIT and CalTech,
electronic voting system expert Rebecca Mercuri revealed that
"the
conclusion that MIT/CalTech researchers has drawn, that
Florida's new voting
technology shows a 35% improvement, is based on a flawed
analysis and is
likely erroneous." She goes on to state that not only are the
researchers
comparing "apples to oranges" in terms of the types of
technologies surveyed
(punch-cards versus optically scanned and DRE machines), but
they have
misleadingly compared Gubernatorial general election results to
Gubernatorial primary results (and only for the Democrats in the
2002
primary).

It is well known that voters in general elections turn out in
far greater
numbers (in Florida it is estimated that the November election
will show a
400% increase or more) than in primaries, putting greater strain
on the
performance of systems as well as on poll workers and voters.
The balloting
style of the typical primary voter (usually a party insider, and
certainly a
partisan with a larger interest in selecting candidates for each
race on the
ballot) is quite different from the general election voter, where
independents and other non-declared or minority party
affiliation citizens
are permitted to cast ballots. Thus, only in November will we
be able to
ascertain whether the residual vote rate has actually
"improved." Hence,
Dr. Mercuri asserts, "the conclusion is premature, as well as

flawed."

Laudatory statements made by Stephen Ansolabehere, Charles Stuart and R. Michael Alvarez regarding Florida's new voting systems are also sorely misleading, and do not support their conclusion of 35% improvement. MIT Professor Stuart's comment that "most of the problems covered by journalists...did not concern equipment malfunctions" is not based on an analysis of the numerous and severe voting system problems that occurred throughout the state, but rather on the media reports that surfaced. Many equipment malfunctions were reported by the Associated Press and other news bureaus, but these were obfuscated by the public interest stories that alternatively showed voters "pleased with the new equipment" or being "turned away from the polls in droves."

A lot of the media attention focused on press comments by Governor Jeb Bush and members of his staff who erroneously characterized the problems as being based only in two counties (Miami-Dade and Broward) and blamed the poll workers and election officials there for the situation. In actuality, Miami-Dade and Broward could not have purchased the ES&S machines had they not been pre-certified by the state for use. Sadly, this certification failed to provide the counties or their poll workers with sufficient notification as to the fact that the voting machines would take 10 minutes to start up, with the ones outfitted for the visually impaired taking an astonishing 23 minutes. Some machines also contained a "safety feature"

that did not permit them to be turned on before 6AM on election day. Since each unit is activated sequentially, simple math shows that a polling place containing 10 voting machines, with one outfitted for the visually impaired, would not be fully operational until nearly 8AM (an hour after the polls opened) under the best conditions. Mercuri states: "I certainly do not see how this can be blamed on the poll-workers, nor how it constitutes an improvement. I'm hard pressed to think of any computer equipment manufactured after the 1970's that takes 23 minutes to be started, especially those deployed for use entirely in time-critical operations. The failure by MIT/CalTech to raise serious concerns about the engineering of these products is remiss."

MIT's Ansolabehere stated that "the machines used showed clear gains over the technologies used in past elections." To which Dr. Mercuri replies: "Yes perhaps, if one considers declaring a state of emergency (under threat of lawsuit by a major candidate) and extending the election day by two hours a "clear gain." How about in Union County, Florida, where 2,700 optically scanned ballots had to be hand counted, because the computers were erroneously programmed to only tally votes for Republican candidates? At least there, the ballots could be recounted because they were on paper. What about the precinct in southern Florida that showed a 1200% voter turnout (12 times as many voters as were registered) because the DRE activation cards permitted voters to cast ballots on machines in the same

building that were not in their precinct? And what about some precincts in Miami-Dade and Broward where the vote cartridges reflected over 40% residual votes (lost or missing) and data had to be "extracted" from back-up memory inside of the machines (one wonders how trusted the reconstructed results can be)?"

CalTech's Alvarez states "we are learning important lessons about how to make such important changes in voting technologies" and Mercuri asks: "Is it fair to allow Florida and other states and communities to feel pressured to replace their voting systems while being treated as guinea pigs? Is the United States prepared to reimburse communities for defective and obsolete equipment once new standards are in place (since all election equipment is still being inspected by the National Association of State Election Directors testing authorities to the outdated 1990 Federal Election Commission guidelines)? Is it acceptable to certify voting equipment that can be reprogrammed internally via a portal on the device (as some were, only weeks before the election in Palm Beach County as well as elsewhere in the state)? These new technologies are playing a role in electing government officials - the confidence citizens have in the democratic process is at stake."

Mercuri, who has testified before the U.S. House Science Committee regarding the need for involvement of the National Institute of Standards and Technologies in establishing criteria for the procurement and

testing of election equipment, feels that congressional election reform is sorely needed. But, she notes that many of the laws proposed at federal and state levels, or enacted since 2000, have been weakly worded so as to permit the production of election equipment that does not provide an independent means whereby voters can verify human-readable ballots that are secured and available for recounts. "Real election reform," Mercuri says, "is only possible within a context of adequate and enforceable standards for construction, testing, and deployment of voting equipment."

But Mercuri worries that the trend to full automation of the voting process could be used to conceal election fraud. She warns, "It is entirely possible that Florida and other states may smooth out their election day problems such that it appears that the voting systems are functioning properly, but votes could still be shifted or lost in small percentages, enough to affect the outcome of an election, within the self-auditing machines. Whether this occurs maliciously or accidentally, it presents a frightening prospect. Thankfully, new products are being developed that provide the voter with a way to determine that their ballot has been tabulated correctly, without revealing the contents of their vote, but deployment of such systems is a few years down the road."

For these reasons, Dr. Mercuri has requested a moratorium on the purchase of any new voting systems that do not provide, at minimum, a voter-verified,

hand-recountable, physical (paper) ballot while appropriate laws, standards, and technologies are developed that will provide accurate, secure, reliable, and auditable voting systems. She urges MIT, CalTech, and other concerned scientists, public officials and private citizens to join her in this cause.

For further information contact:

Rebecca Mercuri, Ph.D.
P.O. Box 1166, Phila. PA 19105
609/895-1375, 215/327-7105
www.notablessoftware.com/evote.html
mercuri@acm.org

✶ Cost cutting endangers hospital power

"Rich Brown" <rabbav@freemars.org>

Sat, 21 Sep 2002 09:07:00 -0500

<http://www.twincities.com/mld/twincities/news/4119286.htm>

[The above URL may disappear before this issue appears.]

There is no individual villain here - it took the combination of a power company willing to reduce reliability in the name of cutting costs and errors installing the (multiple) hospital generators to cut operating room power.

✶ South Wales train leaves without driver

"Fuzzy Gorilla" <fuzzygorilla@euroseek.com>

Wed, 18 Sep 2002 18:39:30 -0400

Another episode of a train leaving the station without its driver occurred on a South Wales commuter train between Rhymney and Cardiff. The driver, who had been chatting with railway workers on the platform, did a 100-yard sprint to catch up with the train. However, a spokesman for Valley Lines reportedly said that the train would have stopped automatically in another fifty yards. [Source: All Aboard! Except for Driver of Runaway Train, Reuters item, 18 Sep 2002, via Yahoo; PGN-ed; perhaps the driver was in training (sprintwise)?]

http://dailynews.yahoo.com/news?tmpl=story2&u=/nm/20020918/od_nm/train_dc

✶ Greek government doesn't quite ban electronic games

Bruce Anderson <bruce-anderson@rogers.com>

Fri, 13 Sep 2002 20:27:30 -0400

This one sounded too far out, so I checked with the local Greek consulate. (My question to them was "is this a hoax?", quoting the Web page referenced in [RISKS-22.23](#).) Here is their reply. I hope this clears the air a bit.

After we received your e-mail we have forwarded it to the Press Office of the Greek Embassy in Ottawa. They have informed us they are

aware of these

articles but they are not accurate. The New Greek Law has banned all games

that can be used for gambling or modified for gambling purposes even if

they exist in private spaces (Only Casinos are excluded from the banning).

However neither foreign tourists neither Greek citizens will be prosecuted

when they use cell phones with games , or lap tops in which games are

installed or any portable game consoles for example :play stations,

gameboys, x-box etc, since these games cannot be modified for gambling and

furthermore the owner doesn't insert coins or credit cards in order to

continue using them. We hope that this answers your question.

⚡ Yet another intrusive Web site

Michael Ortega-Binderberger <miki@ics.uci.edu>

Thu, 12 Sep 2002 02:50:13 -0700 (PDT)

A few days back, and with the september 11 anniversary, a local news station

in Los Angeles, CA (reasonably large audience) advertised the efforts of a

Web site called 4MyEmergency.com. The idea is that most people do not have

all their personal information "together" in case of a disaster, and the

Web site wants to help you get your act together. Its full of good wishes,

privacy pledge, etc. so far so good.

What the Web site does for you is to generate a report that you can leave

with a loved one in case of disaster. Unfortunately, disaster

can come much earlier thanks to its information gathering process. It asks you in a series of 7 forms all conceivable information about yourself: name, address/phone, birthdate, names/phones of family, friends, your doctor, dentist, pharmacist and insurance agent, your medical history, home, car, health and life insurance policies (the company, phone, policy numbers and where they are), home security company and even though they don't "recommend" you give them your security code, yep, there you can write it down if you so choose. To make you feel good, you can also include your religious and pet information to go with your credit card, banking, accountant, attorney and real estate information.

Its actually so concerned with security that it does not ask for your social security number, you can just write it down on the final printout, or "mail it to a friend or family member you trust".

The homepage states that "For additional security, this Web site uses the highest level encryption." However, all of this is transmitted in the clear with not even SSL encryption to a Web site that has no credibility beyond good wishes and a click-through privacy agreement.

To be fair, most fields are optional, but then, why would anyone use it in the first place?

The RISKS? The information they collect is tailor made for identity theft, they have no security, and the media is giving them a free pass and even

some promotion despite frequent warnings about identity theft in southern California.

✶ Air passenger jailed for using mobile

George Roussos <gr@dcs.bbk.ac.uk>
Wed, 11 Sep 2002 16:25:51 +0100 (BST)

A passenger who played a game on his mobile phone during a flight has been jailed for four months. (BBC coverage at: <http://news.bbc.co.uk/1/hi/england/2248683.stm>)

The risks of playing Tetris!

✶ Re: Microsoft says Win 2000 hacking outbreak subsides ([RISKS-22.24](#))

<mike.patnode@teradyne.com>
Thu, 12 Sep 2002 16:28:01 -0400

> MS urges us to take preventive measures to protect themselves against
> future attacks: eliminate blank or weak administrator passwords, disable
> guest accounts, run up-to-date antivirus software, use firewalls to
> protect internal servers, and stay up to date on all security patches.

I just had Windows 2000 installed on my laptop (company policy). This

software ships with very little security enabled and numerous webs sites, including Microsoft, tell me to update it and change account settings. But it is so hard to figure out what to do! We are told to change the Admin password, but also warned that some (unnamed) programs will stop working if we do this. The computer help files and Microsoft web site do not tell which accounts are needed or why. What I can tell is my machine has now been changed into a multi-user environment, which is not what I want. Also Microsoft tells us to use "snap-ins". What on earth are they? Which ones affect which accounts? I can't make random changes to my machine, as it has to work within a corporate network.

I think the reason this is so confusing is Microsoft does not know what are the correct settings for the many pre-installed accounts and is trying to make its users figure this out on their own. Otherwise, wouldn't the software be shipped with appropriate settings already enabled?



✶ Re: The pinnacle of chutzpah in spam filtering

Peter Corlett <abuse@mooli.org.uk>
Wed, 11 Sep 2002 17:05:10 +0000 (UTC)

> [Why you'd have a content filter on an 'abuse@...' is beyond me.]

> [Because they get lots of spam also? PGN]

Yes.

I adopted a username of "abuse" in 1998 or so to reduce the amount of spam I received. It was rather effective. Still, the thieves who want to steal my bandwidth have now added the new address to their "Trillion Guaranteed Addresses" CDs and there's a reasonable chunk aimed at my MX hosts.

The MX hosts run abuse@ through my hand-crafted Exim Filter rules and issue bounces. They're based on header peculiarities caused by certain popular bits of spamware, so the usual risks of keyword filtering don't seem to apply in my specific case. I include a phone number in the bounce, and nobody has complained yet, anyway.

When I used to work on an abuse desk, we had an incredible amount of junk sent to the abuse@ address as well. Unfortunately, it wasn't sensible to attempt to filter that lot, exactly because of the noted RISK. Besides, I wouldn't get the BOFHly pleasure of nuking a user for spamming if I'd lost the complaint :)

✶ Re: Retrospective Karger/Schell paper on Multics Security Evaluation

<karger@watson.ibm.com>

Wed, 25 Sep 2002 17:48:05 -0400

Since our paper was reviewed this week on both RISKS (Summit, [RISKS-22.25](#)), people who downloaded it may be interested in obtaining a newly

revised copy
that includes a few small changes based on some of the comments
and
suggestions we have received, as well as some typographical
corrections.
Roger and I thank everyone who sent us comments (from Slashdot,
RISKS, and
open-source), as they were most helpful.

The URL remains the same:

[http://domino.watson.ibm.com/library/cyberdig.nsf/papers?
SearchView&Query=\(multics\)&SearchMax=10](http://domino.watson.ibm.com/library/cyberdig.nsf/papers?SearchView&Query=(multics)&SearchMax=10)

[http://domino.watson.ibm.com/library/cyberdig.nsf/papers
?SearchView&Query=\(multics\)&SearchMax=10](http://domino.watson.ibm.com/library/cyberdig.nsf/papers?SearchView&Query=(multics)&SearchMax=10)
[broken, if your mailer blows the unbroken version]

Some people downloading it on 24 or 25 September (yesterday and
today) may
have run into problems, both with the link to the actual PDF and
with two
pages being missing from the PDF. Both of these problems have
now been
resolved, and I hope that they did not cause anyone too much
trouble.

★ REVIEW: "Pearl Harbor Dot Com", Winn Schwartau

Rob Slade <rslade@sprint.ca>
Wed, 11 Sep 2002 19:46:31 -0800

BKPRHRDC.RVW 20020628

"Pearl Harbor Dot Com", Winn Schwartau, 2002, 0-9628700-6-4, U
\$9.99

%A Winn Schwartau winns@gte.net

%C 11511 Pine St. N., Seminole, FL 33772

%D 2002
%G 0-9628700-6-4
%I Inter.Pact Press
%O U\$9.99 727-393-6600 fax: 727-393-6361
%P 512 p.
%T "Pearl Harbor Dot Com"

Dear Winn,

Thank you for the copy of "Pearl Harbor Dot Com." In recognition of this book's demonstration of your deep personal commitment to recycling (and at least you admit that this story started life as "Terminal Compromise": many don't) I was going to reprint my original review (cf. BKTRMCMP. RVW) but I suppose that wouldn't be fair to anyone.

You have tightened up the writing considerably. (With age, and a few more books under the belt, comes grammar, eh?) However, I still note "refuse" for "refuge," a semicolon for "that," "hesitancy" for "hesitation," and a whole lot of redundancy. (And what is with your fetish for "Glen Fetich"?)

Your characters are a little more interesting and consistent, although Miles Foster (and most of the other technical people) still seem to be geek wish fulfillment.

The plot has more tension, but it is still **way** too convoluted. You've got a whole shoal of red herrings (and you know what they say about old fish after a while) and a ripped-out wiring closet full of loose ends.

Even disregarding a computer system that will crack Blowfish and AES in seconds, and the wonderful, mythical lethal virtual reality

feedback bug, I still have some technical bones to pick with you. Why does a power outage shut down a battery operated radio? Carbon dioxide does not suck oxygen out of the air. And my son-in-law is a pilot on that type of aircraft, and has had power failures at exactly that point in the flight (the latest due to a lightning strike). My grandchildren aren't orphans yet.

I couldn't ignore your "virus" now, could I? In having it burn out a printer port, were you trying to resurrect the old "Desert Storm virus" canard? I recognized the old timing based video burnout trick and the somewhat debated issue of excessive diskette read head travel (neither was ever used in a virus). But, for crying out loud, if you sold three hundred million "infected" programs, why would you need a virus? And if you distributed that many copies of malware, you think nobody would notice? (Yes, OK, "Windows." Partial point to you. But people are finding bugs in it every day.)

I agree with your basic point: the general public should be more aware of the weaknesses in the technology that controls so much of modern life. But you don't strengthen your argument by making enough mistakes that it looks like you don't understand it either.

copyright Robert M. Slade, 1993, 2002 BKPRHRDC.RVW 20020628
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com
<http://victoria.tc.ca/techrev/~rslade> or <http://sun.soci.niu.edu/~rslade>



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 27

Sat 28 September 2002

Contents

- [Risky Auckland harbour bridge lane signals](#)
[Nickee Sanders](#)
 - [Dewie the Turtle comes out for computer security](#)
[NewsScan](#)
 - [Re: Real risks of cyberterrorism?](#)
[Ralf Bendrath](#)
 - [Probability Risk Assessments/Homeland Insecurity](#)
[Peter B. Ladkin](#)
 - [Paper ballots, no panacea](#)
[Andy Neff](#)
 - [Leeches for Sale](#)
[Rebecca Mercuri](#)
 - [Info on RISKS \(\[comp.risks\]\(http://comp.risks\)\)](#)
-

⚡ Risky Auckland harbour bridge lane signals

Nickee Sanders <njs@ihug.co.nz>
Tue, 24 Sep 2002 11:47:37 +1200

The Auckland harbour bridge is an arched, 8-lane structure, whose inner 4 lanes are employed in a so-called "tidal" system to cope with changing traffic demands.

For decades, control has been achieved by a simple system of lane signals above each lane, every 200m or so: a green arrow if the lane was open to traffic, a red cross if it was closed, and a diagonal arrow if the lane was closing ahead.

Now some bright spark has obviously decided it's much simpler to indicate that a lane is open by having NO SIGNAL AT ALL above it. Shall we open a RISKS sweepstake on how soon it'll be before a power outage causes an accident?

[Fortunately, head-on crashes are prevented by the use of a movable barrier.]

Nickee Sanders, Software Engineer, Auckland, New Zealand

🔥 Dewie the Turtle comes out for computer security

"NewsScan" <newsscan@newsscan.com>
Thu, 26 Sep 2002 10:34:11 -0700

In the tradition of Smokey the Bear's campaign for fire safety, the new cartoon figure Dewie the Turtle is being promoted by the Federal Trade Commission to teach kids and their parents of the importance of computer and

network security (<http://www.ftc.gov/infosecurity>). Dewie urges the selection of hard-to-guess passwords, the use of antivirus software and computer firewalls, and other security practices. Do as Dewie says or you'll be sorry. (*San Jose Mercury News*, 25 Sep 2002; NewsScan Daily, 26 September 2002)

<http://www.siliconvalley.com/mld/siliconvalley/4151919.htm>

[So, Do We Do as Dewie Says? OK, but that is nowhere nearly enough.

But that's just what the recent draft of the President's Critical

Infrastructure Protection Board (CIPB) said *each user* should do.

Unfortunately, the CIPB's recommended 60 measures totally ignore the

reality that most of the computer systems are so lame that those user

measures are still seriously inadequate. Are you Dewie-eyed? Not me.

The Dewie I'd root for would move faster than a turtle. PGN]

✶ Re: Real risks of cyberterrorism? (Norloff, [RISKS-22.22](#))

Ralf Bendrath <bendrath@zedat.fu-berlin.de>

Mon, 23 Sep 2002 22:07:59 +0200

> ... study by the Gartner Group ... not referenced

The non-publication of the Gartner/NWC study is a problem, I agree. At

least, the audio recording of the conference discussing the outcomes

afterwards is available:

http://www3.gartner.com/2_events/audioconferences/dph/dph.html.

But let's talk about what we know from open sources. The outcome of the study was, in my understanding, that the assumption "give me ten hackers, and I'll bring this nation to its knees" is plainly wrong. The U. S. military (including NSA) probably has more experience in offensive computer network attacks (CNA) than any other government body in the world. CNA have been part of the doctrine of "information operations" since 1998 (see Joint Pub. 3-13, Joint Doctrine for Information Operations, http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf) and have been used in Kosovo and on other occasions. The "after action reviews" and people from these units I talked to all concluded that it turned out much more difficult than expected. It takes an immense effort in net intelligence (NETINT), technology and human expertise and manpower to really get some serious damage done.

Therefore, the government cyber threat estimates in the last months (after some hysteria about "cyberterrorism" after 9/11) have been reduced to a more sober assessment. Though I normally am not in line with him, I totally agree with the conclusion Richard Clarke, the White House's cyber security czar, drew after the Gartner/NWC exercise: "There are terrorist groups that are interested. We now know that al Qaeda was interested. But the real major threat is from the information-warfare brigade or squadron of five or six countries." (quoted after Ariana Eunjung Cha / Jonathan Krim, "White House Officials Debating Rules for Cyberwarfare", Washington Post, 22

August
2002).

If you look at the latest National Strategy to Secure Cyberspace, which was released on September 18 (<http://www.whitehouse.gov/pcipb>), in the chapter on threats and vulnerabilities there is one scenario that lists a number of cyber security/computer risks incidents that have already happened:

"Consider the Following Scenario... A terrorist organization announces one morning that they will shut down the Pacific Northwest electrical grid for six hours starting at 4:00PM; they then do so. (...) Other threats follow, and are successfully executed, demonstrating the adversary's capability to attack our critical infrastructure. (...) Imagine the ensuing public panic and chaos." (p. 4)

It clearly looks impressive, but: Many of these incidents have not occurred by purpose, but by plain technical failures. This is not really something any cyber attacker can rely on. And the main example for cyber vulnerabilities and risks in the Strategy are the Nimda and Code Red worms. These kinds of "weapons" can really not be used for any directed attack, and they to my knowledge are not at all capable of spreading to SCADA systems that do not rely on MS Outlook. ;-)

I have just finished a review of the changes in the U.S. cyber threat discourse before and after 9/11, and one conclusion for me was:

"The threat perception can change when the criteria for a threat are

changed. The problem here is: There still are no clear criteria even within government organizations for deciding what is an attack and what is not, and some security agencies tend to overstate the real incidents. Until 1998 the Pentagon counted every attempt to establish a telnet connection (which can be compared with a knock on a closed door) as an electronic attack. Another example shows even better how arbitrary some estimates are. When asked by the Department of Justice about the number of computer security cases in 2000, the Air Force Office of Special Investigations (AFOSI) staff counted 14 for the whole Air Force. The Department of Defense overall count for all services, to the surprise of the AFOSI staff, later summed up to some 30 000. The explanation: The other services had counted non-dangerous events like unidentified pings as hacker attacks, while the AFOSI only had considered serious cases. On the vulnerability side of the problem as well, there are still no standard procedures for identifying and estimating the vulnerability of critical infrastructures. These are being developed since June 2000 in the Critical Infrastructure Protection Office's project "Matrix". Slowly, a discussion seems to emerge on the validity of statistics about the numbers, dangers and damages of computer insecurities. Even Richard Power of the Computer Security Institute that conducts the annual Computer Crime Survey for the FBI was quoted with some self-critical words on this problem. "

(I can send a copy of the full article to anyone interested. It

will be

published this fall as: The American Cyber-Angst and the Real World -

Any Link?, in: in: Robert Latham (ed.): Bytes, Bombs, and Bandwidth, New York: New Press, 2002)

Talking about "cyberterrorism": My problem with many of the publications and

fears about it is the total focus on vulnerabilities. While you can see tons

of quotes from "security professionals" or IT lobbyists on this, you never

find any expert on real-world terrorism being asked about it by the

media. If you try to think from this angle, the threat becomes much smaller:

Terrorists are not used to hacking, and hackers and terrorists are totally

different milieus and cultures. Terrorists don't need to hack, because

low-tech approaches work perfectly well (I just say "boxcutters"). But even

more important: Terrorism is a form of political communication. The

terrorist act itself is not the goal, but the message transported by it and

the psychological impacts. For this, computer attacks are just not "sexy"

enough - you don't get these "great" TV pictures if you bring down a

telephone network or a computer in a satellite control center. So, IMHO

terrorist will use the nets more and more for organisational and communicational purposes, but not for attacks.

So I guess, my main point is: Be aware of the risks related to computer

networking, but do not participate in the fearmongering parts of the media

and some interested parties on Capitol Hill are doing.

✈ Probability Risk Assessments/Homeland Insecurity ([RISKS-22.21](#) to [23](#))

"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>

Wed, 25 Sep 2002 10:02:16 +0200

I'm glad that Stephen Fairfax in [RISKS-22.23](#) considers as a "classic example" my rejection in [RISKS-22.22](#) of his claim in [RISKS-22,21](#) that a probabilistic risk assessment (PRA) finds "overwhelming evidence" that arming commercial pilots is an overall plus. I thank him for that characterisation. I myself didn't rate my note so highly. I hope to do better here.

Fairfax doesn't buy my criticism of his reasoning by a long margin. It seems worth understanding the issue in detail, for two reasons. First, while the topic of arming commercial pilots is only marginally relevant to Risks (in that computerised control systems may be more vulnerable to bullets than hydromechanical systems), the subject of the appropriate application of PRAs is central. It was discussed in Risks eleven years ago inter alia by Hoffman ([RISKS-12.16](#)), Agre ([RISKS-12.21](#), [12.24](#)), Gardner, Seidel ([RISKS-12.22](#)), and Kerns ([RISKS-21.24](#)). Second, I have seen the type of invalid reasoning, exemplified by (**) below, more than once in discussions of PRAs for particular phenomena. It seems useful to put a refutation in the public record.

To the argument.

Fairfax correctly notes that I focus on just one assertion of his, namely that (B): there is "overwhelming evidence" that (A): arming commercial pilots would ameliorate hijacking situations. He wishes us to believe (A) with him on the basis of (B). Indeed, were (B) to be true, we would be irrational not to believe (A). How does he wish us to believe (B)? On the basis (C) of assessing the "probabilities of success and failure"; in short, a PRA.

Let us look at the form of the argument. First, we have the indisputable premise that (A) follows from (B).

Fairfax's argument then continues ostensibly with the form: (*) (C), therefore (B), therefore (A).

But in fact it doesn't have this form, as his reply in [RISKS-22.23](#) makes clear. His argument actually has the form:

(**) If one were to perform (C), one would find (B).
Therefore (A)

That Fairfax hasn't actually performed a PRA (C) is made clear by his comments in [RISKS-22.23](#) about how one would go about doing it. Not: how one actually did it; but, rather: how one would go about doing it were one to do so.

It would be convenient were (**) to be valid under the supposition (=A7). For then we could achieve our desired results, not by actually doing things to achieve them, but simply by imagining the outcomes

were we to do
so. Making wine, bringing up children, winning the Olympics, and
proving
Fermat's Last Theorem would all be so much easier than we had
thought. But
unfortunately it is not so valid.

Fairfax wishes us to believe (A). The reasoning he proposes is
(*). He
himself believes (A) on other grounds, though, for he does not
have the
components of (*); he has at most (**). So the grounds he
actually has for
believing (A) are not the grounds he is proposing that there are
for
believing (A). C.S. Peirce called this "sham reasoning" [1]. I
called it
bogus. Reader's choice.

So much for the general point. I also doubted that the chain of
reasoning
(C, therefore B) could be established, even were one to attempt
it. I said
Fairfax had no data. He disputes that. We have a different
classification of
data. I think that to perform any kind of probabilistic
assessment of the
consequences of arming commercial pilots, he needs at least some
cases in
which commercial pilots have been armed, and as far as we know
there aren't
any. He claims that all he needs are cases of attempted
hijacking. OK, let's
take that at face value and see what we get.

He does note that the data are "sparse". Let me indicate how
sparse.
Aviation Safety Network lists just 16 occasions in the 50 years
before
September 11, 2001 on which aircraft have been lost to hijacking
incidents
[2]. These are the most damaging hijacking incidents in larger
numbers of

lives were lost. Others were more or less successfully concluded. The list is not complete. It omits, for example, one hijacking-to-destruction of a US domestic flight (PSA, a BAe 146 near San Luis Obispo, CA on 12 December 1987 by a passenger with a gun). It also omits three suicide/murder incidents by pilots (one Air Maroc, whose date I do not recall, and two recent ones to a Silk Air Boeing 737 in Indonesia and an Egyptair Boeing 767 off the East Coast of the US. Note that the first is supposed, not proven, and the two latter are so considered by the NTSB but not necessarily by other parties to the investigation). So let's double the number to 30. Can these, *probabilistically*, tell us that arming US domestic pilots will help or hinder? Of course not. There are more potential confounding factors than there are incidents, so it is impossible to control for them, except in the one obvious case of the 4 incidents due to Al Qaeda operations.

That virtually nothing probabilistically follows from these incidents does not mean that they cannot be analysed. One could go through on a case-by-case basis and propose counterfactuals: what do we think would have happened, had the cockpit crew been armed? Indeed, Fairfax proposes something like this. Additional incidents may become appropriate for such an analysis, say the Air Algerie incident which Fairfax notes. But this is not any kind of probabilistic evaluation, let alone a PRA, as proposed in (C). It is a counterfactual case analysis, the typical analysis used in accident investigation of all sorts, and does not have a role to

play in an
argument of form (*).

Fairfax regrets that I didn't consider his "additional layer of safety" argument. OK, I'll bite. First of all, it is a metaphor. Second, I think it is an inappropriate metaphor to describe what is being proposed. The policy of the FAA and US domestic airlines up to now has been "clean aircraft". That is, no anti-personnel weaponry on board (with certain - unloaded - exceptions). The justification is that, if there is none on board, then none can be used. Arming pilots violates this policy. Far from adding an "additional layer of safety", it peels one off and replaces it with another. Besides, third, I don't think evaluating metaphors, mine above included, is an appropriate way to reason in safety cases. Fourth, what about cases in which pilots themselves are the problem (there have been three, at least, as above, fully ten per cent of what I take to be the total if one is impressed by such argument from tiny numbers)? Even the deployment of weaponry on board by trained enforcement agents has had problems which would not occur were the weaponry not to be present [3].

Finally, readers please note that I have neither said nor implied what my considered position on (A) actually is. As I said above, I don't consider it a theme appropriate to the Risks Forum.

Footnotes:

[1] Peirce used the phrase to refer to reasoning to a conclusion to which the proponent is already committed for other reasons. See

Haack, *Manifesto of a Passionate Moderate*, Chicago U.P., 1998, p8ff.

I am using it here to characterise a situation in which the reasons one gives for a conclusion are not the reasons one really has, which is the same thing in other words. Haack was more concerned with the case in which a proponent was committed to a conclusion and would not give it up no matter what. I am not suggesting in any way that this is the case here.

[2] <http://aviation-safety.net/events/seh.shtml>

[3] See Bob Herbert's frightening NYT account of what happened to Dr. Bob Rajcoomar, a retired army major and physician, published in The International Herald Tribune on 24 September, 2002, at <http://www.iht.com/articles/71537.htm> [Also made *TheNYTimes*. PGN]

Peter B. Ladkin, University of Bielefeld, <http://www.rvs.uni-bielefeld.de>

✶ Paper ballots, no panacea

Andy Neff <anef@votehere.net>
Wed, 18 Sep 2002 17:25:36 -0700

In analyzing the recent election failures in Florida, it is important to avoid jumping to erroneous conclusions about the role that machines can play in election systems of the highest quality. There are significant differences between information-based election systems and the simplistic electronic-based systems (often called Direct Recording

Electronics or DREs) generally offered in the market today. Research on information-based voting systems has been conducted since the 1980's. Little, if any, of this research has been incorporated into the electronic voting systems widely used today.

First of all, the vast majority of objections to electronic systems are not directed at fraud, which is actually the biggest weakness of simple DREs. Rather, objections are often directed at issues of reliability and performance. These issues are certainly important to the voting process; however, they can be resolved through proper certification, testing, and training. Such flaws are avoidable and are not problems uniquely associated with voting systems.

Remember the butterfly ballot in Palm Beach County, Florida in the 2000 Presidential Election? This example clearly illustrates that even certified paper-based systems are subject to reliability and performance problems. Justifiable indignation, then, should be focused on the absurdly outdated and ineffective election standards and certification process. Ultimately, it is the job of an unbiased standards organization to enforce minimum reliability and performance policies for election systems.

An unfortunate consequence of belaboring performance issues is that the thorniest election issues are not examined carefully enough. Those against electronic solutions have concluded, without appropriate supporting

evidence, that election systems that use countable paper ballots are most trustworthy.

The fallacy of this conclusion is demonstrated by both the facts that are often given to support the paper ballot solution, and by those that are conveniently omitted:

1) As most who witnessed the 2000 US Presidential Election agree, paper ballots created problems. Paper ballots, be they optical scan or punch card, still have to be counted by machines in an election of any reasonable size. This means that the opportunity for election fraud is not eliminated by the use of paper, but only shifted to a different point in the election process.

2) It is often suggested that electronic voting systems get retrofitted with some form of paper ballot output. I call this the \$2500 #2 pencil solution. Doesn't an electronic machine retrofitted this way remain just as vulnerable to "catastrophic failure," "malfunction," and "usability problems"?

3) While most people intuitively understand how a collection of voted paper ballots could be supervised procedurally, in reality the process is always far from perfect. Even in what was arguably the most scrutinized election in history -- the 2000 US Presidential Election -- ballots were lost, damaged, and/or destroyed. We don't know, and never will know, the extent of the damage; nor will we know how much damage was due to accident and how

much was due to malice. But it is clear that many voters were disenfranchised.

The truth is that paper-based voting systems are "voter verifiable" in that they can help each voter check that his/her choices are recorded properly.

But they are not "publicly verifiable" in that they cannot ensure that the final count is an accurate tally of all the voters' choices.

Simple DRE

electronic voting systems are neither voter verifiable nor publicly

verifiable. Our goal should be to create a system that is both, and modern

information technology gives us this opportunity.

Another common objection raised is the use of "proprietary systems." I

wholeheartedly support this objection. One of the basic tenants of a

trustworthy election system is that nothing should be secret about the

election process except the link between an individual voter and any one

specific voted ballot. Actually, I support something stronger than "open

source," namely "open protocol," which publishes the underlying voting

technology in addition to the software source code.

As Rebecca Mercuri recently said on this forum, "democracy is at stake." I

agree. But I also fear the recommended paper-based solution.

Doctors once

prescribed leeches for deathly ill patients. Sometimes the patients got

better; sometimes they died. In any case, the state of medical science was

not well served by the common wisdom of the time.

C. Andrew Neff, Ph.D., Chief Scientist, VoteHere, Inc.

Copyright (c) C. Andrew Neff, 2002. All rights reserved.

🔥 Leeches for Sale (Re: Neff, [RISKS-22.27](#))

"Rebecca Mercuri" <mercuri@acm.org>

Tue, 24 Sep 2002 00:24:21 -0400

Dr. Neff makes some interesting points but MISSES the point of the paper ballot solution. Here are the facts. DREs fail because of reliability, performance, and security issues, but these can NOT be resolved ENTIRELY through standards and testing. It is a fact of computer science that no manner of testing or code examination can assure software or system integrity. This was explained by Ken Thompson in his classic speech/paper "Reflections on Trusting Trust" (available in its entirety -- at <http://www.acm.org/classics/sep95> -- it's a must read, especially if you believe Open Source is a viable solution to the voting problem).

Neff appears to entirely misunderstand my paper ballot concept. First of all, I have NEVER said that people should go out and spend millions of dollars on expensive paper printers, rather, I have been recommending for years that communities buy simple optical scanning voting systems if they feel they must unload their coffers of the tax dollars they have collected. But the DREs (WITH PRINTERS) can do a better job in preparing the paper ballots, there's no need for blanks prepared in advance, and overvotes and undervotes can be flagged and brought to the attention of the

voters. Where
I see the computers being used with paper is to provide an
ENHANCED voting
system.

For example, Dr. David Chaum has worked out an amazing system,
using
cryptography, where the voter can VISUALLY VERIFY that their
ballot was
cast, the ballot is produced in a form that can not reveal its
contents
(except through a verifiable process that does not identify the
voter), AND
the voter can anonymously verify AFTER the election that their
ballot was
indeed cast as intended. A human-readable physical ballot is
ESSENTIAL to
the process, not only in Chaum's system, but for any electronic
ballot
casting and tabulating device, because it is the ONLY WAY that
the voter can
be assured that their ballot is entered into the count correctly
(no manner
of recording of electronic data will suffice). But the
"paper" (in Chaum's
scheme, laminated plastic, but still a physical audit trail) is
essential to
the process. Once the vendors become willing to admit this is
not possible
without something the humans can actually SEE, they might
finally start
implementing viable systems that are truly auditable. BTW, you
can read all
about Chaum's and my theories in this week's issue of The
Economist.

Dr. Neff is wrong on two more counts. As it turns out, leeches
ARE still
used in medicine. They emit a type of substance that can be
helpful in
certain cases. And actually blood-letting (in modest degrees)
also turns out
to be an effective treatment for some ailments. (There were some

articles on
this a few years back, either in Science News or Smithsonian, I
forget
which, but well documented.) But I think the analogy he made is
quite
apropos to this discussion -- it illustrates a mode of erroneous
thinking
where older technologies (like paper and leeches) are
characterized as
inherently bad, in favor of new- fangled (and occasionally
widely off-base)
solutions.

This is consistent with other VoteHere technology choices --
only a few
years ago, their president, Jim Adler, was pushing Internet
voting. At a
debate sponsored by George Washington University in January 2001
-- the GWU
report (available at www.democracyonline.org) states that --
Adler's team at
Votehere.net "includes scientists who claim they have already
solved many of
the hardest problems associated with Internet voting, namely the
security,
privacy and auditing challenges. For example, addressing the
question about
audit trails, Mr. Adler said that Votehere.net has designed a
system where
votes are "burned onto a cd-rom". Now that's real security for
you.

Thankfully, the NSF decided that Internet voting isn't a good
idea, or the
VoteHere scientists might have sold some of their secure systems
to
Florida. Even Bruce Schneier thinks Internet voting is
implausible, and he
does know a thing or two about crypto.

I could go on further, but my thoughts are embodied in papers on
my website
(at www.notablessoftware.com/evote.html). I commend Dr. Neff on
his

initiative in engaging in this debate. I hope that he might also re-examine the immutable facts of computer science and perhaps he can eventually convince his team of scientists to develop voting systems that are truly verifiable, auditable, and secure. In the meanwhile, I have a few leeches for sale.

Rebecca T. Mercuri, Ph.D., Professor of Computer Science, Bryn Mawr College



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

[ACM](#) Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 28

Monday 7 October 2002

Contents

- [Payroll fail-safes "didn't work"](#)
[J. Lasser](#)
- [Bear Stearns' bare sterns: erroneous order](#)
[David Lesher](#)
- [Raders of the Last Quark](#)
[Identity withheld by request](#)
- [Too fast fingers, or bad shortcut design?](#)
[Pertti Huuskonen](#)
- [Rep. Boucher --finally-- introduces bill to rescind part of DMCA](#)
[Declan McCullagh](#)
- [Defense Information System Agency leaves shopping list online](#)
[PGN](#)
- [Quantum cryptography for secure global communications](#)
[NewsScan](#)
- [Busboy pleads guilty to ID theft](#)
[Monty Solomon](#)
- ["Trojan horse" music?](#)
[Matthew Anderson](#)
- [Court will welcome e-mailed explanations of traffic tickets](#)
[Dave Stringer-Calvert](#)

- [Dewie the Turtle == Bert the Turtle](#)
[Jason T. Miller](#)
 - [Address change blocked by online entry validation](#)
[George N. White III](#)
 - [Batteries: More electronic voting risks?](#)
[anon123](#)
 - [Re: Electronic voting methods](#)
[David Hedley](#)
 - [Re: Paper ballots, no panacea](#)
[David F. Skoll](#)
[Jan C. Vorbrüggen](#)
 - [Re: Butterfly ballots](#)
[George Russell](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ Payroll fail-safes "didn't work"

"J. Lasser" <jon@lasser.org>
Sat, 28 Sep 2002 14:50:16 -0400

<http://www.cnn.com/2002/US/Midwest/09/27/offbeat.teacher.paid.ap/index.html>

The only overpaid teacher, AP item, 27 Sep 2002

A Detroit public school teacher's pay was enough to make Bill Gates or Donald Trump envious. Thanks to a computer glitch, the teacher was paid \$7.9 million before taxes for 18 minutes of work. The teacher, who wasn't identified, received \$4,015,624.80 after taxes. Someone alerted the school district earlier this month, and the money was returned after six days, chief financial officer Ken Forrest said in Thursday's Detroit News.

The error occurred when a clerk entered an employee number in the hourly wage field for the teacher's wage adjustment check. The district's payroll software didn't catch the mistake. "One of the things that came with (the software) is a fail-safe that prevents that. It doesn't work," Forrest said. The district has since installed a program to flag any paycheck exceeding \$10,000, he said.

[Gee, did they test the fix?]

Jon Lasser jon@cluestickconsulting.com

<http://www.tux.org/~lasser/> <http://www.cluestickconsulting.com>

✶ Bear Stearns' bare sterns: erroneous order

David Leshner <wb8foz@nrk.com>

Wed, 2 Oct 2002 23:34:42 -0400 (EDT)

> Bear Stearns placed an erroneous order to sell \$4 billion worth of stock
> late Wednesday at the New York Stock Exchange, but most of the order was
> canceled before it was executed. The NYSE said a clerical error caused
> the brokerage house to enter the order to sell \$4 billion worth of
> Standard & Poor's securities at about 3:40 p.m. -- 20 minutes before the
> stock market closed. The order should have been for \$4 million. All but
> \$622 million of the \$4 billion transaction was canceled prior to
> execution, the NYSE said in a statement. The NYSE had no

further

> comment. Officials at Bear Stearns were not immediately available for

> comment. [AP item]

We have talked about sanity checking time after time. You'd think that a major move would require MULTIPLE management approvals.....but..

We have met the enemy and he is us...

✈ Raders of the Last Quark

<[Identity withheld by request]>

Fri, 4 Oct 2002

A friend is being admitted to a respected eating-disorders clinic in Southern California, which I was interested to learn more about. They have a fantastic supportive Web site at <http://www.raderprograms.com/>, mostly directed at individuals who have plucked up the courage to investigate treatment options.

However, a small slip of the keyboard can destroy that courage. Drop the "s", and <http://www.raderprogram.com/> redirects you to the Web site of Nutri/System --- ``your online weight loss solution'' asking ``how much weight you would like to lose? 10-20 pounds? more than 40?'. Changing `rader' to the more intuitive spelling `radar' gives the same results...

The Nutri/System site seems quite legitimate, and of utility to

a large percentage of the population (pun intended). But to litter the `typo space' in this way is of potentially life-threatening consequence to the individuals seeking the Rader Programs site, and thoroughly immoral.

[Weight! Wait! Don't Spell Me! PGN]

⚡ Too fast fingers, or bad shortcut design?

<pertti.huuskonen@nokia.com>

Mon, 30 Sep 2002 10:27:22 +0300

A colleague recently sent me an e-mail containing material that was clearly not supposed to reach me. Apparently the sender had copied some text from another e-mail, with the intention to sanitize out the unsuitable bits, but had accidentally hit "send" before having completed the edits.

While this certainly happens all the the time and should be no news to any RISKS readers, it did stop me to think about e-mail client UI design.

In our e-mail software, the keyboard shortcut for sending the message out is CTRL-Enter. In our word processing software (from the same manufacturer) the command to delete the last word is CTRL-backspace. The same word deletion method also works in our e-mail client, and seems to get frequent use by many people.

The two keys are rather close together on most keyboards.

Composing e-mail,
I sometimes accidentally hit CTRL-Enter instead of CTRL-
backspace. The
e-mail client then happily sends out the uncompleted e-mail.

Acknowledging my bad keyboard technique, I have chosen to leave
my e-mail
client in an offline mode, so I will have time to go back to my
Outbox to
rescue any stray e-mail before synchronizing with our IMAP
server. I have
therefore had to change my working mode due to the design of
keyboard
shortcuts.

The RISKS? Bad shortcut design coupled with too fast fingers can
cause
embarrassing situations, possibly exposure of improper material,
and
increased global demand for an UNDO feature in sendmail.

⚡ Rep. Boucher --finally-- introduces bill to rescind part of DMCA

Declan McCullagh <declan@well.com>

Fri, 04 Oct 2002 09:02:54 -0700

Here's Boucher talking about this bill as far back as July 2001:
<http://www.politechbot.com/p-02308.html>

I've put the text of the Boucher bill here:

<http://www.politechbot.com/docs/boucher.dmca.amend.100302.pdf>

A similar bill, though not as widely supported, introduced by
Rep. Lofgren
is here:

http://www.house.gov/lofgren/press/107press/021002_act.htm

News article on Lofgren bill:

<http://news.com.com/2100-1023-960531.html>

-Declan

By Declan McCullagh, Staff Writer, CNET News.com, 3 Oct 2002

A proposal to defang a controversial copyright law became public on

Thursday, after more than a year of anticipation and months of closed-door

negotiations with potential supporters.

Formally titled the Digital Media Consumers' Rights Act, the new bill

represents the boldest counterattack yet on recent expansions of copyright

law that have been driven by entertainment industry firms worried about

Internet piracy.

The bill, introduced by Reps. Rick Boucher, D-Va., and John Doolittle,

R-Calif., would repeal key sections of the 1998 Digital Millennium

Copyright Act (DMCA). It would also require anyone selling copy-protected

CDs to include a "prominent and plainly legible" notice that the discs

include anti-piracy technology that could render them unreadable on some

players. [...]

<http://news.com.com/2100-1023-960731.html>

POLITECH -- Declan McCullagh's politics and technology mailing list.

You may redistribute this message freely if you include this notice.

To subscribe to Politech: <http://www.politechbot.com/info/subscribe.html>

This message is archived at <http://www.politechbot.com/>

Declan McCullagh's photographs are at <http://www.mccullagh.org/>

Defense Information System Agency leaves shopping list online

"Peter G. Neumann" <neumann@csl.sri.com>

Wed, 2 Oct 2002 11:12:29 PDT

Faulty access controls open DISA's technology requisition system to snoops. An improperly secured database operated by the U.S. Defense Information System Agency (DISA) allowed Internet surfers to view and place orders for computers, networks, cell phones, software, and other technology used by the military. Before it was locked down over the weekend, visitors to the Web site of DISA's Requirements Identification and Tracking System (RITS) were able to peruse hundreds of requisition documents, such as a \$310,000 order for "new generation STE crypto devices" in support of the Global Command and Control System.

<http://online.securityfocus.com/news/911>

Quantum cryptography for secure global communications

"NewsScan" <newsscan@newsscan.com>

Fri, 04 Oct 2002 08:36:14 -0700

British researchers have been able to use quantum cryptography keys encoded in photons of light to communicate through air for 23

kilometers, and the expectation is that by March of next year this capability will be extended to 1000 kilometers -- far enough to reach all LEO satellites. Because any measure of a photon will alter its quantum properties, quantum cryptography guarantees that any attempt to intercept a message will be evident. (*New Scientist*, 2 Oct 2002; NewsScan Daily, 4 Oct 2002)
<http://www.newscientist.com/news/news.jsp?id=ns99992875>

✶ Busboy pleads guilty to ID theft

Monty Solomon <monty@roscom.com>
Fri, 4 Oct 2002 01:37:45 -0400

A 32-year-old restaurant busboy pleaded guilty on Thursday to pilfering personal and financial data belonging to America's rich and famous, including billionaire Warren Buffett. Abraham Abdallah, a high-school dropout, entered his guilty plea in response to a 12-count indictment charging him with wire, mail, and credit-card fraud, identity theft, and conspiracy -- in what authorities believe is the largest identity theft in Internet history. The federal case accuses Abdallah of using the information as part of a scheme to steal more than \$80 million from individuals, corporations and financial institutions. Although he pleaded guilty, Abdallah told U.S. District Judge Loretta Preska he was not driven by greed. ... Reuters, 3 Oct 2002 <http://news.com.com/2100-1023-960754.html>

[This case was reported originally in [RISKS-21.29](#). PGN]

✶ "Trojan horse" music?

"Matthew Anderson" <MAnderson@gaic.com>

Thu, 3 Oct 2002 08:35:07 -0400

Per an announcement in from Steath MediaLabs, Inc.,
http://biz.yahoo.com/bw/021003/32166_1.html, quote:

"How many unpaid copies of music would you circulate if each contained your own credit-card number?... Built upon a new MS Windows Media-compatible technology... The StealthChannel is capable of stealthily embedding up to 20 kb/s of data into almost any digital audio signal. Embedded data can be anything from images to text to credit-card numbers... In most cases, data hidden in the StealthChannel can be embedded without increasing filesize..."

They go on to mention that this is intended to be used as a "carrot" for those that do authorized copying of music by providing "goodies" such as discounted tickets or a couple of chapters of books yet to be published... It doesn't take much imagination to see the risks of this technology... Music companies "releasing" singles that when executed, check for other "unauthorized" music files and then delete them or at least send a list back to the music company for legal prosecution, Songs released to Kazmaa or

Gnutella that have viruses embedded in them, etc.

The only limitation (currently, wait till future releases of MS Media players) is that you need the Stealth MediaLab plug-in to execute these "goodies". Ah, to go back to the good old days of having to worry only about subliminal messages and what the music said when play backwards...

M@ Anderson, Enterprise Architect, American Financial Group
580 Walnut Street, Cincinnati, OH manderson@gaic.com (513) 412-4457

🔥 Court will welcome e-mailed explanations of traffic tickets

Dave Stringer-Calvert <dave_sc@csf.sri.com>

Wed, 02 Oct 2002 11:01:06 -0700

Tell it to the judge - or better yet, e-mail it to the judge. County officials are setting up a program under which people who get traffic tickets can e-mail their excuses and explanations to a judge. Until now, they'd have to sit for hours in court, waiting for a hearing. So far this year in the county, there have been more than 1,200 people who want to explain to a judge the circumstances surrounding their traffic tickets. After reading the e-mails, the judges will send their reply - either by e-mail, or an old-fashioned postcard.

<http://www.nandotimes.com/technology/story/555311p-4377123c.html>

[Mike Hogsett asked,
"How long until someone writes the automated excuse
generator? And
starts collecting stats for them so that only the successful
ones are
used?"]

✶ Dewie the Turtle == Bert the Turtle

<jasomill@theoneview.com>

Mon, 30 Sep 2002 08:56:42 -0500 (EST)

Looking at Dewie the Turtle ([RISKS-22.27](#)), I can't help but be reminded of Bert the Turtle from "Duck and Cover" (available at <http://www.archive.org/movies/details-db.php?collection=prelinger&collectionid=19069>). As a matter of fact, looking at the "totality of security measures" taken since September 11th, I can't help but be reminded of "Duck and Cover"; "what has changed" since that fateful day is of no more importance to the "security" of this nation or its people than the bombproof school desks of yesteryear.

In re Dewie, I notice the essential difference between cyber security and civil defense in light of the atomic bomb -- since there was nothing a young child could reasonably do to mitigate the risk of atomic attack, it is reasonable to "at least calm their nerves", at the very least it does no harm. In the case of cyber security, from the perspective of someone who sees so much of IT as fundamentally insecure, providing such a "false

sense" of the same seems ill-advised, as it encourages us to deny the causes of our problems rather than to fix them (standard practice in the computer industry, but practice that will have to change if we're going to materially improve IT security) -- in other words, to "cure the symptoms" while leaving the disease untouched.

The same could of course be said about US "antiterrorism" policy in general, but RISKS is of course not the place for such a discussion.

Jason T. Miller, One View Engineering 317-915-9039 ext. 302

[URL also noted by Richard Akerman. PGN]

✂ Address change blocked by online entry validation

"George N. White III" <aa056@chebucto.ca>

Thu, 3 Oct 2002 22:16:48 -0300 (ADT)

Canada Post recently changed my home mailing address. Previously my address involved a rural route number and mail was addressed to the town in which the post office was situated. The new address has the same street and number, but omits the rural route designation and has a different town and postal code. This change was first announced over a year ago, but the new postal codes were only announced a few weeks ago, and are "official" on Oct. 21, 2002.

BC (before computers) I would simply have mailed change-of-address cards that take only minutes to fill out. Now I have a choice. I can

spend minutes
online trying to find an actual mailing address, or minutes
filling out an
online form, only to find that the new address fails the online
entry
validation when I submit the form.

Many of the companies I deal with, including well-known online
retailers,
allow customers to update their personal information online. In
one case,
when I clicked "submit", the result was an error page stating
that my postal
code was not valid for my street address. After contacting
customer
support, I was told that I could bypass the checks by submitting
the form a
second time.

The risks here are from data validation systems which assume
that there is a
unique mapping (e.g., between street address and postal code)
and can only
be updated at a single point in time, so users will be making
updated
entries before the database has been updated, or will fail to
make the
update so their records become "invalid" when the mapping is
updated.
During a transaction, a mailing address is required when the
order is
placed. Credit card companies may check the shipping address
when the
charge is applied, hopefully not long before when the item is
ready to ship.

My new postal code is interesting, as it consists entirely of
pairs of
easily confused letters and numbers: "2Z", "3B", and "6G". Was
this
error-prone code rejected when postal codes were first issued,
and then
pressed into service when a new code was required? It will be

interesting to
observe how often errors are made by people manually
transcribing the values
I entered in WWW address forms into their mailing databases.

George N. White III <aa056@chebucto.ns.ca>
Head of St. Margarets Bay, Nova Scotia, Canada

⚡ Batteries: more electronic voting risks

<anon123@japan.com>

Tue, 01 Oct 2002 13:44:34 -0700

Office evacuated when box of batteries explodes

A box of recycled nickel-cadmium batteries used in voting machines exploded at a county building Monday afternoon. No one was injured, but about 30 employees were evacuated from the Elections Office at 40 Tower Road.

Around 3:30 p.m., the box of about 1,100 button-shaped batteries blew up, scattering small metal pieces 10 to 15 feet in all directions of the warehouse where they were stored, according to Capt. Gary So of the California Department of Forestry.

So theorized that some of the used batteries had charges left and when their negative terminals touched, heat built up and they exploded.

<http://www.bayarea.com/mld/mercurynews/news/local/4187348.htm>

✉ Re: Electronic voting methods ([RISKS-22.25](#) and 27)

David Hedley <dhedley@hebdenbridge.u-net.com>

Sun, 29 Sep 2002 11:06:05 +0100

Re: Paper ballots, no panacea (Neff, [RISKS-22.27](#))

Andy Neff states in [RISKS-22.27](#) "Paper ballots ... still have to be counted by machines in an election of any reasonable size."

Not so. British elections still [mostly] consist of voters manually entering 'X' in a box adjoining the candidate's name on a sheet of paper. For each constituency [ranging from 1,000,000 eligible voters in a European election to 1,000 in town elections] these sheets of paper are then brought together and counted manually. Candidates (or their agents) are allowed to observe the process.

[Also noted in the UK by T Panton. in provincial and federal elections

in Canada by Charles Cazabon, and David Skoll (next). PGN]

Being a human process, mistakes will of course be made. If the final totals are close, the losing candidate may request a recount. Manual recounts will continue until everyone is satisfied. In extreme cases where candidates are separated by 1 or 2 votes, there will be several recounts.

It's old technology and not very flashy, but it's demonstrably accurate and foolproof.

However the government is now going down the road of making voting sexier by trying out new-fangled (even online) voting methods. I fear the worst ...

RE: Elections In America - Assume Crooks Are In Control (Landis, [RISKS-22.25](#))

Lynn Landis stated in [RISKS-22.25](#) "As far as we know, some guy from Russia could be controlling the outcome of computerized elections in the United States."

She is partially correct. I say "As far as I know, some guy from the United States could be controlling the outcome of computerized elections in the United States."

For many of us in Europe, the US voting system lost all credibility in the last presidential election.

✈ **Re: Paper ballots, no panacea (Neff, [RISKS-22.27](#))**

"David F. Skoll" <dfs@roaringpenguin.com>

Sun, 29 Sep 2002 00:46:35 -0400 (EDT)

"Paper ballots, be they optical scan or punch card, still have to be counted by machines in an election of any reasonable size."

This is manifestly not so. Paper ballots can easily be counted by hand, providing enough people do the counting. The proper way to count ballots is to have officers and witnesses count the ballots for each

polling station,
and then send their totals to regional tallying centers. These regional
centers add up the votes and send their totals to national
centers. By
having a tree of counters, and officials from all interested
parties at each
stage, truly huge numbers of votes can easily be counted by
humans.

If the election is close or results are contested, then the paper
ballots are available for recounting. A human recount of all
ballots
may be slow, but it wouldn't be needed most of the time.

Paper-based solutions can be badly designed, as Neff points out,
but a
well-designed paper solution is about the best we have, in spite
of modern
technology.

✉ **Re: Paper ballots, no panacea (Neff, [RISKS-22.27](#))**

"Jan C. Vorbrüggen" <jvorbrueggen@mediasec.de>
Mon, 30 Sep 2002 18:11:07 +0200

> 1) As most who witnessed the 2000 US Presidential Election
> agree, paper
> ballots created problems. Paper ballots, be they optical scan
> or punch card,
> still have to be counted by machines in an election of any
> reasonable
> size.

There was a general election in Germany a little more than a
week ago. From
61 million eligible voters out of a population of a little over
80 million,

79% or about 48 million actually voted, each having two votes. I think this qualifies as "reasonable size".

The ballot is one piece of paper, on which one has to make a mark in each of two columns. Thus, about 48 million sheets of paper were counted entirely by hand, although I'm sure the tallying above the level of the voting locale is done electronically (this is logarithmic in the number of votes counted in any case). Usually, it takes about six to seven hours to arrive at the "vorläufige amtliche Endergebnis" - roughly, the "provisional official final result". This time, due to some of the election officials leaving their job when it was half done, it took almost ten hours to get to that point. Cost: about one Euro (approx. one US dollar) per eligible voter.

I see no reason to believe that this isn't applicable to almost all types of election. Even the most complicated of elections in Bavaria, where the voter has a large number of votes he can distribute, or not, according to certain rules to those wanting to be elected, take at most two days to get to the final result - the main effect is that the number of invalid ballots is much larger than the usual ~1%, and here a computerized system would surely be able to help in filling out the form according to the rules.

Jan Vorbrüggen - MediaSec Technologies, Berliner Platz 6-8, D-45127 Essen
+49 201 437 52 52 <http://www.mediasec.com>
jvorbrueggen@mediasec.de

Re: Butterfly ballots (Neff, [RISKS-22.27](#))

George Russell <ger@tzi.de>

Mon, 30 Sep 2002 13:43:21 +0200

> Re: Paper ballots, no panacea
> Remember the butterfly ballot in Palm Beach County, Florida ...

I think what the butterfly ballot problem indicates is that ballot papers should be designed for humans, not machines. I have voted in both the UK and Germany, and I think I am not alone among Europeans in finding the current American debate surreal. We all have systems where ballot papers have two columns, with the candidates' names and/or parties listed in the first column, and boxes next to these names in which you put a cross or (for STV systems) a number. All votes are counted at least once, by humans, and (at least the UK) the candidates are entitled to send along representatives to watch every stage of the process. Where there is a problem which might affect the result of an election it ends up in the courts; for example a few years ago a local election turned on whether someone who had put a gigantic cross over the entire ballot paper intended to vote for the candidate whose box contained the centre of the cross, or just intended to spoil the paper. But this is so rare it hardly ever happens. The system is so obvious and so simple it is embarrassing to have to spell it in comp.risks, but I can't understand why American states instead seem addicted to mechanical solutions which will invariably go wrong somehow.

Furthermore I just don't see the point of letting machines do the counting, but keeping backup paper ballots for humans to count just in case the machines go wrong or one of the candidates smells a rat. Why keep paper ballots unless you have trained and experienced humans in place to count them? And if you have that, why not just get the humans to count the papers in the first place? In the UK if the candidates dispute the result of a close-run election they can call for a recount. This is I think much quicker than the original count, since the ballot papers are already sorted, and it is only a question of checking that they are all correctly distributed. I'd have to check the Guinness Book of Records for this, but I think the record number of counts in a British General Election is something like 7, and it took about 20 hours from when the polls closed. A far cry from Florida in 2000, where it wasn't possible to count every vote even once in several months.

I suppose American states choose to do counting by machines because it's cheaper. But you'd think that given that we only vote once every few years, it might be worth spending a dollar or two per voter (I doubt if it costs anything nearly as much as that in the UK) to see that you get every vote counted properly.

I don't want to pretend the British system is perfect; you have other issues like the security problems allocating postal votes in the 2001 General Election, and the risk that, because there is no British

identity card, it is very easy to vote pretending to be somebody else. But these are orthogonal to the question of how you actually vote and count the votes.

I'm not an expert at all. I feel incredibly naive. But at least would someone be good enough to explain in baby-talk why it is necessary to have complex mechanical systems at all, when the simple paper one seems to work so well.

[Incidentally, the butterfly ballot is apparently technically illegal in Florida, but was approved anyway. PGN]



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

[ACM](#) Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 29

Wednesday 9 October 2002

Contents

- [Police close fake online bank](#)
[Dave Stringer-Calvert](#)
- [Risks of automatic Windows updates, and HIPAA legality](#)
[Allan Engelhardt](#)
- [Weak encryption kills wolves](#)
[Urban Fredriksson](#)
- [Microsoft says 1% of bugs cause half of all software errors](#)
[Henry Baker](#)
- [BugBear steals lead from klez in virus prevalence](#)
[Security Wire Digest](#)
- [No-fly blacklist snares political activists](#)
[Tim Meehan](#)
- [Phone system could have your number](#)
[Mark White via Dave Farber](#)
- [Prediction: e-mail will become double-trouble in 3 years](#)
[NewsScan](#)
- [Gender: Unknown -- the risks of perception](#)
[Chris Leeson](#)
- [Re: Too fast fingers, or bad shortcut design?](#)
[Greg Searle](#)

- [Re: Address change blocked by online entry validation](#)
[Chris Smith](#)
 - [Re: Butterfly ballots and other election stuff](#)
[David Olsen](#)
[Leonard Erickson](#)
 - [REVIEW: "Information Security Management", Gurpreet Dhillon](#)
[Rob Slade](#)
 - [2003 IEEE Symposium on Security and Privacy, Call for Papers](#)
[Steve Bellovin](#)
 - [Info on RISKS \(comp.risks\)](#)
-

🔥 Police close fake online bank

Dave Stringer-Calvert <dave_sc@cs.sri.com>
Tue, 08 Oct 2002 19:32:13 -0700

British police on Tuesday said they uncovered a fake Internet bank used to con at least two people out of nearly \$100,000. The National Criminal Intelligence Service (NCIS) said the Web site had been set up using a domain name very similar to that of "a major British bank" and appeared almost identical. "It looks very professional," said a spokesman, declining to name the bank involved because the investigation is still ongoing. "There's also a reputation issue to think of and the issue of trust online."

<http://zdnet.com.com/2110-1106-959644.html>

<http://news.bbc.co.uk/2/hi/technology/2308887.stm>

🔥 Risks of automatic Windows updates, and HIPAA legality

Allan Engelhardt <allane@cybaea.com>

Mon, 07 Oct 2002 19:55:09 +0100

A recent article in InfoWorld discusses Microsoft Windows Service Packs in the context of health care providers.

<http://www.infoworld.com/articles/op/xml/02/09/16/020916opwinman.xml>

Apparently, the latest Service Packs for the popular Microsoft Windows 2000 and XP operating systems contains new licence language that allows Microsoft to install new updates on your machine at will and without notifying you.

The RISKS of having your computer systems changing on their own accord should be obvious. As the article points out, this "upsets many companies whose PCs can't be allowed to morph at will". Indeed.

The article quotes a systems manager at a teaching hospital:

"Our procedures sometimes involve surgery to place over 100 recording electrodes in the patient, sometimes on the surface of the brain. These PC-based systems use Microsoft Windows..."

Having a Windows application controlling the voltage to 100 pins surgically embedded in your brain is scary enough, but what happens if it updates to the latest Service Pack and that causes the systems to fail? While the pins are in your brain...

The article makes the further point that, from 14 Apr 2003, it may be illegal under the Health Insurance Portability and

Accountability Act
(HIPAA) to install Windows Service Packs. In a strange twist,
it may also
be illegal not to install the Service Packs...

See <http://www.hipaadvisory.com/regs/HIPAAprimer1.html> for more
information
on the HIPAA.

The article concludes:

"It's not just hospitals but every user of Windows who should
be
wondering. You'd think Microsoft would understand that
customers don't
want their mission-critical systems changing in the dead of
night. This
isn't brain surgery."

Allan Engelhardt <http://cybaea.com/>

Weak encryption kills wolves

Urban Fredriksson <griffon@canit.se>

Mon, 07 Oct 2002 18:02:51 +0200

Well, of course it's really hunters who do it, but there are
strong
indications they've been helped by weak encryption. In 1998 40
Swedish
wolves, out of about 100, were fitted with transponders in order
to track
their movements to learn more about how wolves reestablish a
presence. Of
them, 20 are still alive, 11 have been found dead with working
transponders,
one has been found dead as a result of illegal hunting without
transponder

and eight (four this summer) have disappeared. That that many transponders have failed is considered very unlikely. Current plans are to quickly replace the transponders to something "not everyone can triangulate". It's not clear from the article in Dagens Nyheter what sort of encryption is used now, but it's clear from the context transmissions has to be coded and that one was aware from the beginning wolf-haters would like to take advantage of the tracking equipment.

Microsoft says 1% of bugs cause half of all software errors

Henry Baker <hbaker1@pipeline.com>

Thu, 03 Oct 2002 12:05:00 -0700

I was shocked, shocked, to hear this stunning statistic! I was also shocked, shocked, to hear that pi was irrational, that the world was round, and that the Beatles had split up.

Microsoft says 1 percent of bugs cause half of all software errors

Reuters, 2 Oct 2002

One percent of the bugs in Microsoft Corp.'s software cause half of all reported errors with 20 percent of bugs responsible for 80 percent of the mistakes, Chief Executive Steve Ballmer said on 2 Oct 2002. Microsoft has been criticised for unstable and unwieldy software -- which runs on more than 90 percent of personal computers. "Let's acknowledge a sad truth about software: any code of significant scope and power will have bugs in it,"

Ballmer told customers in a memo similar to one by Chairman Bill Gates this year renewing Microsoft's commitment to trustworthy computing.

But Ballmer said Microsoft was arming itself with better information to help develop its software, by building error reporting features into its products. Engineers use the reports, sent in a short burst over the Internet, to track software bugs and provide a fix, he said. "We've been amazed by the patterns revealed in the error reports that customers are sending us. About 20 percent of the bugs cause 80 percent of all errors, and -- this is stunning to me -- one percent of bugs cause half of all errors."

While reassuring users the information was used for no other purpose than to fix bugs, Ballmer said such information was shared with other makers of software and hardware to try to improve Microsoft's products. He said Microsoft would work to better the system. "As we understand more errors, we're adding an option for customers to go to a Web site where they can learn more about and even fix the errors they report. In the future we want to enable customers to look up the history of their error reports and our efforts to resolve them."

http://biz.yahoo.com/rc/021002/tech_microsoft_ballmer_1.html

⚡ BugBear steals lead from klez in virus prevalence

<Security_Wire_Digest@bdcimail.com>

Thu, 03 Oct 2002 01:00:00 -0500

By Shawna McAlearney, SECURITY WIRE DIGEST, 4, 74, OCTOBER 3, 2002 [excerpt]

First found circulating in the wild last Sunday, the W32.BugBear worm has raced to the top of virus prevalence lists, displacing Klez for the first time since its discovery last April.

"BugBear is increasing steadily in volume and spreading like Klez, which became the biggest virus ever," says Alex Shipp, senior antivirus technologist at MessageLabs. "Each day, we're seeing more of BugBear all around the world--at least 1,000 copies an hour. It could very well grow to become as big a problem as Klez has been and has gotten firmly entrenched in the home user population."

Similarities to Klez include the use of inconsistent body text, attachment names and subject lines, as well as forged e-mail addresses.

BugBear exploits an unpatched Microsoft vulnerability. After infection, the worm copies itself into the Windows system directory and start-up folder as an executable file with a random three-letter name. It installs a Trojan keystroke logger and attempts to disable antivirus and firewall software. BugBear also attempts to infect other networked PCs via the address book and network shares.

"BugBear is another example of a worm written with instructions to kill an extremely long list of security apps," says Steven Sundermeier, product

manager at Central Command. "The idea of terminating various AV and personal firewall applications is becoming increasingly popular among virus authors."

On the brighter side, Shipp says the BugBear worm could have been much worse.

"We haven't found any remote control facilities yet, which makes the virus less dangerous than it could be otherwise," Shipp says. "Our analysis isn't complete yet so we can't say for certain that it doesn't have that capability, but it appears unlikely."

Antivirus experts recommend updating AV signatures; blocking all Windows programs at the e-mail gateway, if possible; and deploying updated versions of Outlook, Explorer and Outlook Express.

<http://www.message-labs.com/viruseye/report.asp?id=110>

<http://www.microsoft.com/technet/security/bulletin/MS01-020.asp>

To SUBSCRIBE to Security Wire Digest, go to:

<http://infosecuritymag.bellevue.com>

✶ No-fly blacklist snares political activists

"Tim Meehan - OCSARC" <tim@ocsarc.org>

Tue, 1 Oct 2002 12:40:42 -0400

<http://www.sfgate.com/cgi-bin/article.cgi>

?file=/chronicle/archive/2002/09/27/MN181034.DTL

A federal "No Fly" list, intended to keep terrorists from boarding planes,

is snaring peace activists at San Francisco International and other U.S. airports, triggering complaints that civil liberties are being trampled. [...] Critics question whether Sister Virgine Lawinger, a 74-year-old Catholic nun, is the kind of "air pirate" lawmakers had in mind when they passed the law. Lawinger, one of the Wisconsin activists stopped at the Milwaukee airport on April 19, said she didn't get upset when two sheriff's deputies escorted her for questioning. [Source: Alan Gathright, *San Francisco Chronicle*, 27 Sep 2002]

Tim Meehan, Communications Director
Ontario Consumers for Safe Access to Recreational Cannabis Web:
ocsarc.org

⚡ Phone system could have your number (Mark White via Dave Farber's IP)

"Peter G. Neumann" <neumann@csl.sri.com>
Tue, 8 Oct 2002 9:08:44 PDT

>From: Mark White <tausyankee@optusnet.com.au>

Phone system could have your number
Kate Mackenzie, *The Australian*, 7 Oct 2002

A single telephone number doubling as an e-mail address could soon be available in Australia despite fears the technology could become a de facto identification number. Under the ENUM system being analysed by the Australian Communications Authority, one number could track down

a person
via a home or mobile phone number, or an e-mail or website
address. The
technology has attracted controversy overseas because of privacy
implications of people being identified by a single number.

The ACA wants feedback on a discussion paper it has issued,
saying privacy
is one of its concerns. But ACA numbering manager Neil
Whitehead said
potential benefits of the system could be enormous. "People
would only need
to remember one number to contact other people in a variety of
devices," he
said. Equipment manufacturers and Internet service providers
were keen to
pursue the technology.

Telstra proposed a single-number service in 1997 and offered
numbers
beginning with 0500 that could redirect to any number. Called
Telepath, the
service, which cost \$7 a month, failed to attract many
subscribers. ENUM
would have to be deployed across all telecommunications and
Internet
providers to be effective.

IP Archives at: <http://www.interesting-people.org/archives/interesting-people/>

✶ Prediction: e-mail will become double-trouble in 3 years

"NewsScan" <newsscan@newsscan.com>
Mon, 30 Sep 2002 08:36:11 -0700

IDC, the technology research firm, is predicting that within
just three

years, the number of e-mail messages sent worldwide will increase from the current level of 31 billion daily to more than 60 billion daily. Most of it will be spam (unsolicited commercial messages), and if the problem of spam is not dealt with by more effective message-filtering, the usefulness of e-mail as an effective business and personal communications tool will be endangered. IDC executive Mark Levitt says, "Like water flowing out of a hose, e-mail has the potential to fill our inboxes and workdays, overwhelming our abilities to navigate through the growing currents of content." [VNUNet 30 Sep 2002; NewsScan Daily, 30 September 2002] <http://www.vnunet.com/News/1135485>

✶ Gender: Unknown -- the risks of perception

"LEESON, Chris" <CHRIS.LEESON@london.sema.slb.com>
Wed, 2 Oct 2002 16:53:00 +0100

An interesting juxtaposition of "Design" and "User Perception".

I had to visit one of our local hospitals. I went to Reception and identified myself to the receptionist. She asked if I had filled in the Questionnaire (in effect, the Personal Details form) and I hadn't.

She brought out her copy of the form, which had been partially filled in by the administrator who made the original appointment.

It started with the following information:

Name: Andrew Leeson [Andrew being my first name]
Gender: Unknown

Our reactions to this little piece of data were quite different:

Her reaction was to mutter darkly about the administrator who could not tell that "Andrew" was clearly "Male".

My reaction was that:

- (a) The database designer had understood that it was possible for the gender to be unknown (at least at the time the appointment was set up), and chosen suitable values for the field: male, female and (default) unknown.
- (b) In the absence of supplied information, the administrator had not assumed that any one name implied a specific gender.

So, the system was designed correctly, the administrator used it correctly, but the receptionist interpreted it as "bad" because the result was not what she thought of as reasonable.

The actual event - wrong gender data - is not much of a risk. The difference in perception could be.

✉ Re: Too fast fingers, or bad shortcut design? (Huuskonen, [R-22.28](#))

<Greg Searle>

Wed, 09 Oct 2002 12:14:35 -0400

Note also that the shortcut for inserting a "hard return" in a formatted e-mail is Shift-Enter. This is sometimes necessary for, say, creating a multiple-line item in a bulleted list. You can easily send your partially-complete e-mail instead of inserting a hard return just by accidentally misplacing one finger a little lower on the keyboard.

Send any responses to [greg_searle\(at\)hotmail\(dot\)com](mailto:greg_searle@hotmail.com).

[Re: Address change blocked by online entry validation \(White, R-22.28\)](#)

"Chris Smith" <smith@canada.com>
Wed, 9 Oct 2002 11:27:45 -0400 (EDT)

Hopefully those mailing databases are configured to catch transcription errors for Canadian postal codes. In all of the above examples, transcription errors would likely result in the erroneous code failing the standard test of ANA NAN (letter-number-letter number-letter-number) that covers all Canadian postal codes. Further reduction in undetected transcription errors is achieved by disallowing certain letters: Q U O I D F are not permitted in Canadian postal codes. I suspect that Q O D are just too similar to sort out, U is too much like V, F confuses the issue with E, and a plain I (straight vertical stroke) is easily confused with parts of letters like T and L. Some of these may be driven by the requirement to determine postal codes on mail by scanning and recognizing handwritten

codes.

It's important to know what RISK-reducing features are available - and then take advantage of them. Better yet would be a snippet of javascript to check the postal codes before the WWW address form is even submitted.

✶ Re: Butterfly ballots and other election stuff (Russell, [RISKS-22.28](#))

David Olsen <olsen@rational.com>
Tue, 08 Oct 2002 16:50:57 -0700

The messages about elections in Britain and Germany where the ballots are counted by hand seem to indicate (though it wasn't entirely clear) that each ballot contains only one or two races. I agree that in this case hand counting is quite feasible. But in the United States, that assumption does not hold.

As a resident of Portland, Oregon, I get to vote for all of the following elected positions: US president, US senator, US representative, state governor, state senator, state representative, secretary of state, state attorney general, state treasurer, state labor commissioner, state superintendent of schools, state supreme court judges, state appeals court judges, state circuit court judges, regional government commissioners, county commissioners, county sheriff, city mayor, city council members,

school board members, and the water & soil conservation district directors.

Not all of these positions are up for election at the same time, but in the

general election in even numbered years a majority of them are.

In addition

to candidates, I also get to vote for or against any changes to the city

charter or state constitution, any property tax levies, any laws referred to

the voters by the state legislature (usually to avoid the governor's veto),

and any initiatives that citizens have put on the ballot by submitting

enough signatures.

In the November 2000 general election I had about 45 things to vote for on

my ballot. When all the various cities, special districts, and state

legislature districts are factored in, the county elections board had a

total of 117 different races for which it had to count votes in that

election.

I am by no means an election expert, but here are my opinions anyway: It

seems to me that counting every one of those races by hand would be much

slower, more tedious, and more error prone than counting them by machine. I

think the best way to cast and count votes is to have the voter fill in

ovals on a piece of paper, have an optical scanner read the ballots and

count the votes, and have any recounts done by hand. That seems to provide

the best combination of ease and accuracy of voting, quick counting of

results, and verifiability of results when disputes arise.

David Olsen <olsen@rational.com>

[The alternative that makes a single-issue piece of paper possible is that you vote for your delegated representative, and everything else follows therefrom. You are describing the other extreme. PGN]

✉ Re: Butterfly ballots (Russell, [RISKS-22.28](#))

Leonard Erickson <shadow@krypton.rain.com>
Tue, 8 Oct 2002 18:43:59 -0800

Well, as an example, here in Oregon, we can vote by *mail* in most elections. But the votes cannot legally be counted until 8 pm on election day. You can vote as late as that by dropping off the ballot at a collection site!

That means *millions* of votes have to be counted in a few hours.

> Why keep paper ballots unless you have trained and experienced humans in place to count them? And if you have that, why not just get the humans to count the papers in the first place?

Time. We can't *afford* that many people, nor do we have that many trained volunteers available. So if it *does* come down to a manual count, it'll require recruiting and training a *lot* of people.

> I'd have to check the Guinness Book of Records for this, but I think
> the record number of counts in a British General Election is
> something like 7, and it took about 20 hours from when the

polls

> closed. A far cry from Florida in 2000, where it wasn't possible to
> count every vote even once in several months.

Much of this was due to court fights. And the fact that the (poorly designed) ballots were hard to make out the vote on. They had to stop the count several times, and then restart it. Often with changes in the rules as to what constituted a "valid" vote ("hanging chad", "dimpled chad", etc)

Also, look up the population of Florida and compare it with the population of Britain.

[More on multiple races and issues...] My "ballot" for one election a while back was both sides of *six* sheets of paper. With something like six "columns" of things to vote on.

Our ballots are the type where you use a pencil to fill in an oval. The technology for scanning those is something like 40 years old. It's pretty mature and reliable.

And I'm told that any questionable ballots get kicked out to be looked at by a human.

Even so, it only takes a few hours to run the ballots for a major election in the Portland Metro area.

It's not perfect. But I think it's a pretty good compromise between speed, usability and security.

Leonard Erickson (aka shadow{G}) shadow@krypton.rain.com

[Further comment on long US ballots from Andrew Sapuntzakis.

PGN]

★REVIEW: "Information Security Management", Gurpreet Dhillon

Rob Slade <rslade@sprint.ca>

Fri, 13 Sep 2002 12:48:08 -0800

BKINSCMN.RVW 20020628

"Information Security Management", Gurpreet Dhillon, 2001,
1-878289-78-0, U\$69.95

%A Gurpreet Dhillon

%C 1331 E. Chocolate Ave., Hershey PA 17033-1117

%D 2001

%G 1-878289-78-0

%I Idea Group Publishing

%O U\$69.95 800-345-4332 fax: 717-533-8661 cust@idea-group.com

%P 184 p.

%T "Information Security Management: Global Challenges in the
New

Millennium"

This is a collection of essays by different authors. The preface, however, states that the intention was to bring together diverse views and yet to "build an argument." What the argument, or central thesis, of the work is, has not been stated.

Chapter one is supposed to set forth the new challenges to information security, but ends up telling us, at great length, that "the times they are a-changin." (Extracting further information from the academic-speak is not made any easier by the many grammatical oddities and awkward constructions.) Policy is central to security, and so it

is no surprise to see it as the topic of chapter two. What is astounding is the fact that so much is wrong with this paper that it is hard to know where to start. Everything seems to be backwards. It is stated that an audit should be done as the prelude to policy development, by how can you conduct an audit with no policy to measure compliance against? Again, the essay says that the procedures in place will form the policy, whereas it should be the policy that guides development of procedures. A simplistic discussion of ethics makes up chapter three. There really isn't any analysis: after a few facile presentations of both sides of a variety of issues the author just asserts that X is or is not moral. Chapter four is supposed to argue that ethical policies build trust and trust promotes e-commerce, but instead actually just lists a number of random security topics. A look at "cyber terrorism," in chapter five, seems to consist only of listing Web sites for known terrorist organizations.

Prescription

fraud is never rigorously defined, so it is hard to say whether the technical measures proposed in chapter six are relevant or not. Chapter seven tells us (surprise, surprise) that disaster recovery planning is often done inadequately, or left undone. A discussion of development models, in chapter eight, seems to be so abstract that it is of no digital use. Internet and e-business security touches on some miscellaneous subjects in chapter nine. The author obviously thinks Compliance Monitoring for Anomaly Detection (CMAD, with some kind of trademark symbol appended to it) is vitally important, but

chapter ten's explanation seems to just describe another type of statistical change measurement. Chapter eleven vaguely discusses some of the security issues involved with the use of agent or mobile software. The final chapter lists some "motherhood" security principles.

One of the interesting, and disturbing, aspects of the book is that each paper is accompanied by a bibliography of sources, but almost none of the standard security reference works in the various fields addressed are cited. How can you discuss, for example, computer ethics without having read Deborah Johnson's (cf. BKCOMPETH.RVW) works?

Compilation works tend to be hard to pin down, and to vary in quality and usefulness. This work has a remarkable consistency, in that the items included are all vague, uninteresting to the professional, and unhelpful to the practitioner.

copyright Robert M. Slade, 2002 BKINSCMN.RVW 20020628
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

<http://victoria.tc.ca/techrev> or <http://sun.soci.niu.edu/~rslade>

2003 IEEE Symposium on Security and Privacy, Call for Papers

Steve Bellovin <smb@research.att.com>

Tue, 08 Oct 2002 01:33:22 -0400

2003 IEEE Symposium on Security and Privacy

11-14 May 2003, The Claremont Resort, Oakland, California, USA

sponsored by
IEEE Computer Society Technical Committee on Security and Privacy
in cooperation with
The International Association for Cryptologic Research (IACR)

Paper submissions due: 6 Nov 2002

Panel proposals due: 6 Nov 2002

5-minute abstracts due: 17 Mar 2003

For submission guidelines see

<http://www.research.att.com/~smb/oakland03-cfp.html>

For questions, please contact the program chairs, at
oakland-chairs03@research.att.com.

Symposium Committee:

General Chair: Bob Blakley (IBM Software Group - Tivoli Systems,
USA)

(bblakley@us.ibm.com)

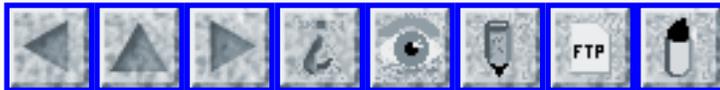
Vice Chair: Lee Badger (Network Associates Labs, USA)

Program Co-Chairs: Steven M. Bellovin (AT&T Research, USA)

David A. Wagner (University of California at Berkeley, USA)

Steve Bellovin, <http://www.research.att.com/~smb>

[This has been probably the most important research conference
on security and privacy for over two decades. PGN]



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

[ACM](#) Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 30

Tuesday 15 October 2002

Contents

- [\\$34M fails to fix DC payroll computers](#)
[David L. Matthews](#)
- [Man dies after playing computer games non-stop](#)
[Mike Hogsett](#)
- [My dishplayer and my digital phone don't play well together](#)
[William Colburn](#)
- [Pac*Bell menu](#)
[Dave Stringer-Calvert](#)
- [The democratic principle and "client-side" denial-of-service](#)
[Andrés Silva](#)
- [Hazards of online translation and plagiarism](#)
[George Mannes](#)
- [Lying 'Lie Detectors'](#)
[William Safire via Monty Solomon](#)
- [Risk of chaining substitutions](#)
[Mich Kabay](#)
- [Nigerian use of technology in elections](#)
[Fuzzy Gorilla](#)
- [Re: Butterfly ballots and electronic counting](#)
[George Russell](#)

[Toby Gottfried](#)

[anon123](#)

[Tony Finch](#)

[David Damerell](#)

[Scott Nicol](#)

● [Re: Weak encryption kills wolves](#)

[Ulf Lindqvist](#)

[Erling Kristiansen](#)

● [REVIEW: "Information Warfare", Michael Erbschloe](#)

[Rob Slade](#)

● [DIMACS Workshop on Software Security](#)

[Gary McGraw](#)

● [Info on RISKS \(comp.risks\)](#)

✂ \$34M fails to fix DC payroll computers

"David L. Matthews" <dml@wam.umd.edu>

Mon, 14 Oct 2002 09:51:59 -0400 (EDT)

Washington DC officials spent more than \$20 million transferring payroll data for city employees cutting over to a new computer system (Comprehensive Automated Personnel and Payroll System) from a 33-year-old system that had a long history of inaccurate and late paychecks. After a year, the new system was no better, so they then spent another \$14 million reverting back to the old system. [PGN-ed] <http://www.washingtonpost.com/wp-dyn/metro/>

[This saga is not atypical of other cases noted here previously,

but RISKS readers will find many lessons of what NOT to do in the

Post article. PGN]

⚡ Man dies after playing computer games non-stop

Mike Hogsett <hogsett@csl.sri.com>

Wed, 09 Oct 2002 18:21:56 -0700

A 24-year-old South Korean man (identified only as Kim, a very common Korean name) was found dead in an Internet cafe after playing computer games nonstop for 86 hours, apparently without sleep or meals. [PGN-ed]

<http://www.smh.com.au/articles/2002/10/10/1034061260831.html>

⚡ My dishplayer and my digital phone don't play well together

William Colburn <schlake@nmt.edu>

Mon, 14 Oct 2002 14:29:36 -0600

For my telephone needs I have a Nokia 6190 with firmware V5.53. For my television needs I have Dishnetwork Dishplayer running at whatever version they last pushed to it. I have known for a while that my telephone and my dishplayer have an "interaction". When I am about to receive a call, the audio on my television has a modem-like sound buried in it. Similar sounds come up periodically when the telephone is sitting idle as well, probably some kind of background communication between it and the tower.

Yesterday, while I was watching the Discovery Channel, an

emergency came up
and I had to make some phone calls. I moved into the next room
with my
telephone. After a little while of talking on the phone, and
making several
different calls, my phone suddenly synchronized with the
Discovery Channel.
The audio track that I could hear from the next room was also
being played
over my telephone. I tried telling the person I was talking to
what had
happened, but when I talked the telephone amplified my own voice
over its
speaker (but not on the television). I I hung up and redialed,
but my
telephone continued to play the Discovery Channel to me. I had
to power
cycle my telephone to make it stop. The person I was talking to
knew that I
had hung up on them, but hadn't heard anything unusual.

If it happens again, I think I'll try changing channels on the
television to
see what happens. Maybe I can get the audio track to a channel
I'm not
subscribed too! :)

The risks here, are that wireless devices could someday/somehow
use the
wrong radio signal and do bizarre and unexpected things.

⚡ Pac*Bell menu

Dave Stringer-Calvert <dave_sc@csl.sri.com>
Mon, 14 Oct 2002 13:13:54 -0700

Less than sane pacbell menu system:

"If you have a dead line, and cannot make calls, press 1"

<press 1>

"If you are calling from the line you are having problems with,
press 1,
else press 2" [...]

⚡ The democratic principle and "client-side" denial-of-service

=?ISO-8859-1?Q?Andr=E9s?= Silva <asilva@fi.upm.es>

Thu, 10 Oct 2002 10:50:00 +0200

Extracted from "Hacktivists target trade summit":

<http://www.wired.com/news/print/0,1294,43137,00.html>

A coalition of cyber-protesters plan to flood 28 websites associated with this weekend's free trade negotiations at the Summit of the Americas with page requests and e-mail messages. ... Dorothy E. Denning, a computer crime and security expert at Georgetown University, thought the group deserved to be regarded as a political, rather than a criminal, organization. "They operate openly and publicly," Denning said. "They also try to operate by a democratic principle, meaning lots of people have to protest to make it effective." She was impressed when the group cancelled a cyber-protest over genetic engineering that had failed to get majority support in an online vote.

In an effort to disassociate themselves from the "server-side" denial-of-service attacks that took down Yahoo and eBay last year, the electrohippies call their technique a "client-side" denial-of-

service
attack.

The difference, according to an electrohippie essay called Occasional Paper No. 1, is that client-side actions require thousands of individuals (clients) using their PCs to participate in order to be effective, while it only takes one person to launch a server-side attack. This is the "democratic principle" that impresses Denning.

Andrés Silva

<http://www.ls.fi.upm.es/UDIS/miembros/asilva/index.html>

⚡ Hazards of online translation and plagiarism

<George.Mannes@thestreet.com>

Wed, 9 Oct 2002 18:30:16 -0400

The original correction, from a student newspaper at Washington State

University:

http://www.dailyevergreen.com/nn4/news/index.asp?Story_ID=6923&StoryPage=1

The Daily Evergreen would like to sincerely apologize for an injustice served to the Filipino-American, Spanish-speaking and Catholic communities on the front page of Thursday's Evergreen. The story "Filipino-American history recognized" stated that the "Nuestra Senora de Buena Esperanza," the galleon on which the first Filipinos landed at Morro, Bay, Calif., loosely translates to "The Big Ass Spanish Boat." It actually translates to

"Our Lady of Good Peace."

Parts of the story, including the translation above, were plagiarized from an inaccurate Web site.

October is Filipino-American History Month. Members of the Filipino-American Student Association of WSU will hold events to celebrate their history and culture all month. They should be able to celebrate without gross inaccuracies and poor coverage by the Evergreen.

We hope these groups accept our deep regret.

The explanation, from the *Seattle Times*:

http://seattletimes.nwsourc.com/html/localnews/134551307_wsublunder09m.html

George Mannes www.thestreet.com 1-212-321-5208 george.mannes@thestreet.com
14 Wall Street - 15th Floor / New York, NY 10005

Lying 'Lie Detectors'

Monty Solomon <monty@roscom.com>

Fri, 11 Oct 2002 17:12:20 -0400

Lying 'Lie Detectors', William Safire, *The New York Times*, 10 Oct 2002

Longtime readers of this column have noticed some recurring themes: I'm for personal privacy and have an affinity for the often-betrayed Kurdish people. I despise state-sponsored gambling as well as the form of torture that calls itself the "lie detector."

Win some, lose some. Losses: Lawmakers are playing the slots, and privacy has been taking a beating from both government and private snoops. But some wins: The Kurds we protect in northern Iraq are united and ready to join in a fight for freedom. And this week, the polygraph -- that hit-and-miss machine measuring sweat, speedy heartbeat and other signs of nervousness -- has been discredited as the judge of truth-telling.

After 19 months of study, experts convened by the National Research Council, an arm of the prestigious National Academy of Sciences, concluded that "national security is too important to be left to such a blunt instrument," and noted pointedly that "no spy has ever been caught [by] using the polygraph." ...

<http://www.nytimes.com/2002/10/10/opinion/10SAFI.html>

✶ Risk of chaining substitutions

"Michel E. Kabay" <mekabay@cs.com>
Fri, 11 Oct 2002 12:17:50 -0400

OBSERVATIONS: A message to one of my students bounced because his e-mail service refused the large attachment I had sent him.

He gave me a different e-mail address to use. I dutifully entered it into the TO: field in my e-mail client and sent him the file again.

That message bounced and I noticed that it had gone to the original address instead of to the desired address.

ANALYSIS: Had I simply written the wrong address into the TO field?

Investigation revealed that the e-mail client I am using (Outlook 2000 SR-1 v 9.0.0.4527) cheerfully looked up the e-mail address in my contact list, found it as his secondary e-mail address, converted the secondary address into my student's name, then converted the name into his primary address.

These conversions were done entirely without visible notification. This sequence of events is repeatable.

WORKAROUND: Right-clicking on the student's name in the TO field did bring up a little menu that allowed me to force the secondary address to be used.

INTERPRETATION: My guess is that (1) Someone decided that when one types a name into the TO: field, it's helpful to look up the e-mail address and plug it into place while still showing the name; thus a name becomes underlined when there's a match. So far so good: very useful and unobjectionable.

(2) Someone (else?) decided that the opposite change would also be useful; i.e., if one writes an e-mail address into a destination field, the program automatically looks it up and shows the underlined name instead of the address. Also reasonable.

(3) Now a tricky bit: someone decided to allow multiple e-mail addresses in the Contact list. However, the conversion from a name into an e-

mail

address always uses the **preferred** address -- and there is no notification of this choice. Also reasonable, albeit on shakier grounds. After all, if there is a preferred address, we ought to use it, right? And if we need to change it, presto! There's a pop-up menus that lets us choose from the alternate addresses. Great! Works fine.

(4) Ah, now we hit pay dirt: someone decided to allow steps (2) and (3) to work in sequence without user intervention. And there we have it: typing an alternate address into a destination field silently converts it to the **wrong address**.

LESSONS FOR DESIGNERS:

1. If you override your users' inputs and propose to change their entry to what you think is better, tell them you're doing so and let them refuse the change.
2. Don't link a series of operations together without thinking about the consequences of that chain of operations.

M.E. Kabay, PhD, CISSP, AssocProf InfoAssur, Dept CompInfoSys, Norwich University, Northfield VT mkabay(at)norwich(dot)edu

[Typo **preferred** fixed in archive copy. PGN]

Nigerian use of technology in elections

"Fuzzy Gorilla" <fuzzygorilla@euroseek.com>

Fri, 11 Oct 2002 11:32:32 -0400

Nigerian officials are investing \$30 million in technology (including BioLink fingerprint scanning) in hopes that next April's presidential election -- their first under a civilian government in 42 years of statehood -- will be peaceful. A trial run in late September resulted in riots after would-be voters were informed there were no more registration forms (apparently having been hoarded by lower-level officials -- 70M were printed for 60M supposed eligible voters), with reports of shootings, lootings and takeovers of government and business facilities as well. The fingerprints will hopefully prevent voters registering more than once, especially with multiple identities. [Source: Nigeria Vote: Peace Through Tech? Michelle Delio, Lycos/wired.com, 11 Oct 2002; PGN-ed]

<http://www.wired.com/news/politics/0,1283,55702,00.html>

[Perhaps the Nigerians are still using the old African technique of putting a pebble into one of several competing jars. Assuming no fraudulent pebbles are introduced and the pebbles are all similarly sized if you want to avoid actually counting them, that scheme might actually be more trustworthy than all-electronic voting in the absence of any assurance that your vote will be counted correctly (as noted previously in RISKS). The pebble scheme is clearly not rock-et science, but the opportunities for rocking the ballot box still seem to be considerable. But the idea of using biometrics in the voting process may merely move fraud around to other parts of the process, especially if the

other parts
are inherently not trustworthy. PGN]

[Incidentally, PGN asked our long-time election technology expert on this subject to comment. This was her response:]

Not only that, but this also brings up a lot of human rights issues.

Sure, "democracies" might want us to ante up our biometrics to the government for the "privilege" of voting. Makes one almost want to live in a dictatorship! Rebecca Mercuri

⚡ Re: Butterfly ballots and electronic counting (Erickson, [RISKS-22.29](#))

George Russell <ger@tzi.de>
Thu, 10 Oct 2002 10:54:12 +0200

Remind me, how much did the Presidential candidates in 2000 spend on television advertising again? Don't you think it might have been better to have spent, say, 10% of that on getting the votes counted properly?

⚡ Re: Butterfly ballots and electronic counting (Erickson, [RISKS-22.29](#))

"Toby Gottfried" <toby@gottfriedville.net>
Thu, 10 Oct 2002 19:35:42 -0700

>That means *millions* of votes have to be counted in a few hours.

"have to be"?

Only because our society (mainly the news media) is obsessed with instant gratification.

Oh, the horror of going to bed on election night not knowing ... not finding out until the next morning or the day after that ... the uncertainty ... the waiting ... what ever would we do ?

Most US elections don't take effect until at least a couple of months later (November to January for national elections).

Out of those 60 or so days, I could spend the first two or three not knowing an election outcome. Unfortunately, the TV news people can't.

✶ Re: Butterfly ballots (Russell, [RISKS-22.28](#))

<anon123@japan.com>

Wed, 09 Oct 2002 14:31:43 -0700

The California Constitution puts the burden for counting votes on the voter, not the government:

SEC. 2.5. A voter who casts a vote in an election in accordance

with the laws of this State shall have that vote counted.

RISK of poorly worded laws? "A voter...shall..." vs. "the state shall count

that vote."

✶ Re: Butterfly ballots and other election stuff (Olsen, [RISKS-22.29](#))

Tony Finch <dot@dotat.at>

Thu, 10 Oct 2002 15:09:30 +0100

In the UK each elected position has its own ballot paper, so you will often have to mark more than one piece of paper at the polling station. This allows the votes for each post to be counted in parallel, and it means that recounts can be done efficiently because counting for the second post does not mess up the sorting of the ballot papers for the first post.

✶ Re: Butterfly ballots

David Damerell <damerell@chiark.greenend.org.uk>

Thu, 10 Oct 2002 12:32:31 +0100 (BST)

>Also, look up the population of Florida and compare it with the >population of Britain.

OK... Florida's population is about 16 million. Britain's population is about 60 million. So I'm not sure what the point is here, especially since our counting system would scale perfectly well to a population of 600 million.

The solution to the long ballot problem is surely to put the important selections on a separate ballot that can be easily hand-counted, and let the (existing, well-understood) machines deal with the assistant dog-catchers and whatnot.

David Damerell <damerell@chiark.greenend.org.uk>

✶ Re: Butterfly ballots

Scott Nicol <snicol@apk.net>
Thu, 10 Oct 2002 00:47:51 -0400

The US has about double the per capita GDP of Britain. If the Brits can afford it, the US certainly can. As for trained volunteers, you'd have them if you recruited and trained them. It's got to be less effort than what is put into the census.

[Scott also noted the relative populations... PGN]

✶ Re: Weak encryption kills wolves (Fredriksson, [RISKS-22.29](#))

Ulf Lindqvist <ulf@sdl.sri.com>
Wed, 9 Oct 2002 16:59:07 -0700 (PDT)

The original article in **Dagens Nyheter** does not mention encryption per se and there is no indication that any encryption has been broken

(the phrase "broken the code" is probably used in a very generic sense). The statement that anyone could triangulate the current transmitters makes me suspect that they are either (a) not even transponders, but transmit a signal at regular intervals, or (b) simple transponders that are activated by a simple tone signal or similar. In case (a), encryption of the signal content would not prevent triangulation of the radio signal by unauthorized parties. In case (b), encryption of the activation signal would make it harder for the hunters to activate the transponder, unless replay attacks were possible. Of course, as long as it is active, anyone could triangulate the transponder.

What would be a better system, from the point of view of the wolves and the researchers? If the wolves could be fitted with GPS receivers, the transmitter could use encryption and more advanced radio techniques to send its position to the authorized receiver, as no triangulation would be needed.

Ulf Lindqvist, System Design Lab, SRI International, 333 Ravenswood Ave, Menlo Park CA 94025-3493, USA +1 650 859-2351 <http://www.sdl.sri.com/>

✉ Re: Weak encryption kills wolves (Fredriksson, [RISKS-22.29](#))

Erling Kristiansen <erling.kristiansen@xs4all.nl>
Sun, 13 Oct 2002 20:17:02 +0200

It seems to me that encryption is not really the issue here. Encryption could hide the identity of a particular wolf, but would not hide the radio signal as such. There is likely to be very few radio transmitters in "wolf country", so if you find a signal on the right frequency, it is likely to come from a wolf transmitter.

What is called for is a means to make detection of the signal itself difficult/impossible. Spread spectrum techniques spring to mind: By spreading the radio signal over a wide frequency spectrum, detection is impossible unless you know how the spreading was done, and are able to "de-spread" the signal. In other words, you hide the signal in the noise for anybody not having the code to extract it.

Spread spectrum is used in military systems for exactly this reason. (And used in mobile telephony, but for other reasons that are not relevant to this subject)

🔥 REVIEW: "Information Warfare", Michael Erbschloe

Rob Slade <rslade@sprint.ca>
Tue, 8 Oct 2002 12:42:20 -0800

BKINFWFR.RVW 20020721

"Information Warfare", Michael Erbschloe, 2001, 0-07-213260-4, U \$29.99

%A Michael Erbschloe
%C 300 Water Street, Whitby, Ontario L1N 9B6
%D 2001
%G 0-07-213260-4
%I McGraw-Hill Ryerson/Osborne
%O U\$29.99 800-565-5758 905-430-5134 fax: 905-430-5020
%P 315 p.
%T "Information Warfare: How to Survive Cyber Attacks"

In both the preface and the introduction, the author makes a point of stating that this book is different from others in the field, that it does not simply use the old military paradigm to analyze information warfare, and, as a result, will be more useful to business. It is, therefore, rather startling to find, in chapter one, background basics that stick strictly to the military model. Everything is presented purely from the perspective of single attacker and single defender, and it's definitely black hat versus white. The model thus constructed is weak in several areas, and would not seem to be able to even address a number of issues. For example, writers such as Dorothy Denning (cf. BKINWRSC.RVW) postulate the potential harm that can arise from corrupted data and other misinformation, which may be used for purposes ranging from propaganda to degrading decision systems. And what do we do about business situations, where today's colleague may be tomorrow's competitor? Chapter two uses profligate verbiage to list a few points about economic impacts that will come as no surprise whatsoever to anyone with the slightest background in business impact analysis. In chapter three, Erbschloe turns to fiction. He proposes a scenario in which

a gang of cyber-terrorists causes one trillion dollars worth of damage. In doing so, the author demonstrates that a) his experience in information warfare is limited to viruses, b) his experience with viruses is limited to Loveletter, and c) he believes all the movie stereotypes about "hackers."

Black hat communities are seldom as cosmopolitan as the one proposed. They are never as original: multiple viruses based on the model used would quickly be caught by generic means. It is also a lot easier to write simple virus variations than it is to break into specific targeted systems for specific targeted information.

We are told, in chapter four, that in order to fight against the information warfare threat, all governments and militaries must get together. (Can we hear a chorus of "And do it my way!" swelling in the background?) Then we have a relay of military strategies in chapter five. Supposedly chapter six turns to corporate strategies, but with the emphasis on terrorists and the FBI, we seem to be back to the military again. A number of tables are used to assert that terrorists and rogue criminals are interested in attacking various industries. (Proof of these statements seems to be singularly lacking.) Chapter eight lists companies proposed to be in the "information warfare" reserve: able to provide expertise in the event of an attack. In light of the recent business debacles, these lists unintentionally provide some of the most humorous reading in the book. (For those who know the security problems of some of these companies, the lists are even

funnier.)

Tellingly, the material on the civilian "casualties" of infowar, in chapter nine, is the most restricted in the book. Chapter ten seems to move into fiction again. Erbschloe, without much in the way of evidence, says that the "geek in the basement" brigade is now about to turn pro, en masse. (He also states that we are going to have a skilled and active black hat population of 600,000 by 2005.) The statement, in chapter eleven, that we need more skilled law enforcement people is unsurprising, and also unhelpful. The conclusion, in chapter twelve, that we need more money and attention for security is equally useless.

This is a verbose reiteration of minor points that are evident to anyone with any background in security, let alone specialists in the information warfare field. Mind you, the book was probably not intended for experts. However, readers with no knowledge of data security are likely to be misled. They will feel that they have been taught about information warfare. They haven't.

copyright Robert M. Slade, 2002 BKINFWFR.RVW 20020721
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

<http://victoria.tc.ca/techrev/~rslade> or <http://sun.soci.niu.edu/~rslade>

⚡ DIMACS Workshop on Software Security

Gary McGraw <gem@cigital.com>

Wed, 9 Oct 2002 17:20:39 -0400

Dates: January 6-7, 2003

Location: DIMACS Center, CoRE Building, Rutgers University

Organizers:

Gary McGraw, chair, Cigital, gem@cigital.com

Ed Felten, Princeton University, felten@cs.princeton.edu

Virgil Gligor, University of Maryland, gligor@umd.edu

Dave Wagner, University of California at Berkeley, daw@cs.berkeley.edu

Invited Speakers:

* Brian Kernighan, Princeton University:

Coding Excellence: Security as a Side Effect of Good Software

* Michael Howard, Microsoft:

The Microsoft Trustworthy Computing Initiative from the Inside

* Dan Geer, @STake:

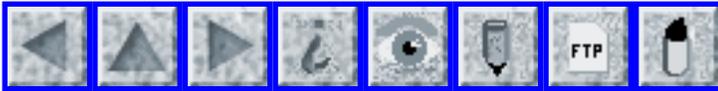
Software Security in the Big Picture: Repeating ourselves all over again

WWW Information: <http://dimacs.rutgers.edu/Workshops/Software/>

The security of computer systems and networks has become increasingly limited by the quality and security of the software running on these machines. Researchers have estimated that more than half of all vulnerabilities are due to buffer overruns, an embarrassingly elementary class of bugs. All too often systems are hacked by exploiting software bugs. In short, a central and critical aspect of the security problem is a software problem. How can we deal with this?

The Software Security Workshop will explore these issues. The scope of the workshop will include security engineering, architecture and implementation risks, security analysis, mobile and malicious code, education

and training,
and open research issues. In recent years many promising
techniques have
arisen from connections between computer security, programming
languages,
and software engineering, and one goal is to bring these
communities closer
together and crystallize the subfield of software security.



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

[ACM](#) Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 31

Monday 21 October 2002

Contents

- [E-ZPass Users in New Jersey Will Get Replacement Devices](#)
[Monty Solomon](#)
- [The high risk of low security: element 118](#)
[Wendell Cochran](#)
- [Password complexity -- not just for computers anymore](#)
[Seth Arnold](#)
- [GPS: Keeping Cons Out of Jail](#)
[Monty Solomon](#)
- [How mobile phones let spies see our every move](#)
[Monty Solomon](#)
- [Airline Security](#)
[Morten Welinder](#)
- [GAO: Commercial Satellite Security Should Be More Fully Addressed](#)
[Monty Solomon](#)
- [UCSD bans WinNT/2K -- will it do any good?](#)
[Jeremy Epstein](#)
- [Outlook knows best!](#)
[Jim Bauman](#)
- [Microsoft Skins a Knee on the Astroturf](#)
[Monty Solomon](#)

- [Bogus Yahoo e-mail picks up credit-card numbers](#)
[Tom Van Vleck](#)
 - [A new twist to Bugbear](#)
[Paul Edwards](#)
 - [How we run elections in the UK](#)
[Richard Pennington](#)
 - [Re: Risks of automatic Windows updates, and HIPAA legality](#)
[Chuck Karish](#)
[Greg Searle](#)
[Douglas Siebert](#)
 - [Re: Pac*Bell menu](#)
[Crispin Cowan](#)
 - [Re: Hazards of online translation and plagiarism](#)
[Bob Schuchman](#)
 - [Re: Weak encryption kills wolves](#)
[Phil Smith III](#)
 - [Peter L. Bernstein, Against the Gods: The Remarkable Story of Risk](#)
[PGN](#)
 - [REVIEW: "Hacking Exposed", Stuart McClure/Joel Scambray/George Kurtz](#)
[Rob Slade](#)
 - [REVIEW: "Have You Locked the Castle Gate", Brian Shea](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ E-ZPass Users in New Jersey Will Get Replacement Devices

Monty Solomon <monty@roscom.com>

Wed, 16 Oct 2002 03:39:36 -0400

New Jersey's E-ZPass windshield transponders are wearing out sooner than expected, resulting in hundreds of thousands of mistaken violation notices being issued. Similar problems with the manufacturer, Mark IV Industries,

have arisen in 14 states (not all of which are E-ZPass customers). Over about 900,000 users out of six million will be getting free replacements.

[Source: Ronald Smothers, *The New York Times*, 16 Oct 2002, PGN-ed]

<http://www.nytimes.com/2002/10/16/nyregion/16PASS.html>

[Head them off at the Pass? PGN]

✶ The high risk of low security: element 118

Wendell Cochran <atrypa@eskimo.com>

Wed, 16 Oct 2002 11:01:13 -0700

Recently a prominent physicist at the Lawrence Berkeley National Laboratory was fired, and the reported detection of element 118 was retracted.

Everyone concerned agrees that essential data in a computer file had been faked, forged, or fudged.

[What to name the would-be new element?
Phonium? Phakium? Phorgium? Phudgium? PGN]

The fired physicist denies doing the dirty work. According to *The New York Times, Science section, 15 Oct 2002: ``He says he is as perplexed as anyone. His account on the laboratory computer system was used by everyone in his group, he says, and his password was an open secret.''

Sardonic cackling in the deep background may emanate from the ghost of Richard P. Feynman, once the resident lockpicker at Los Alamos.

Wendell Cochran, West Seattle

✂ Password complexity -- not just for computers anymore

Seth Arnold <sarnold@wirex.com>

Sat, 19 Oct 2002 17:15:15 -0700

The outside key-code on my building has five buttons but ten digits -- two digits per button. This allows for 10^n different "combinations" as humans must remember it, but 5^n different combinations as the door remembers it.

Who thought of this? Hopefully the same person who thought capitalizing all passwords before performing comparisons was a good idea -- I'd hate to think there are more than a handful of people making mistakes like this.

✂ GPS: Keeping cons out of jail

Monty Solomon <monty@roscom.com>

Tue, 15 Oct 2002 19:48:51 -0400

An electronic tracking system that follows suspects and criminals around their neighborhoods and compares the information to current crimes has received, of all things, the stamp of approval from the American Civil Liberties Union. The Global Positioning System's satellites track

probationers and parolees and compare their whereabouts to the location of crimes committed in their vicinity. ... [Source: Julia Scheeres, wired.com, 15 Oct 2002]
<http://www.wired.com/news/privacy/0,1848,55740,00.html>

✶ How mobile phones let spies see our every move

Monty Solomon <monty@roscom.com>
Tue, 15 Oct 2002 20:18:45 -0400

Government's secret Celldar project will allow surveillance of anyone, at any time and anywhere there is a phone signal

Jason Burke and Peter Warren, 13 Oct 2002, *The Observer*

Secret radar technology research that will allow the biggest-ever extension of 'Big Brother'-style surveillance in the UK is being funded by the Government. The radical new system, which has outraged civil liberties groups, uses mobile phone masts to allow security authorities to watch vehicles and individuals 'in real time' almost anywhere in Britain. The technology 'sees' the shapes made when radio waves emitted by mobile phone masts meet an obstruction. Signals bounced back by immobile objects, such as walls or trees, are filtered out by the receiver. This allows anything moving, such as cars or people, to be tracked. Previously, radar needed massive fixed equipment to work and transmissions from mobile phone masts

were thought too weak to be useful. ...

http://www.observer.co.uk/uk_news/story/0,6903,811027,00.html

✈ Airline Security

Morten Welinder <terra@diku.dk>

15 Oct 2002 21:04:26 -0000

Finally someone in FAA and in the mainstream press [ahem] has gotten a clue and figured out how to improve airline security. If only all these airline security articles had anything to do with comp.risks.

Seeking to address "the number-one threat to airline security," the

Federal Aviation Administration announced Monday that it will consider

banning passengers on all domestic and international commercial flights. [...]

http://www.theonion.com/onion3838/faa_passenger_ban.html

✈ GAO: Commercial Satellite Security Should Be More Fully Addressed

Monty Solomon <monty@roscom.com>

Fri, 18 Oct 2002 01:19:56 -0400

GAO: Commercial Satellite Security Should Be More Fully Addressed

<http://www.gao.gov/new.items/d02781.pdf>

UCSD bans WinNT/2K -- will it do any good?

"Jeremy Epstein" <jepstein@webmethods.com>

Thu, 10 Oct 2002 08:06:55 -0400

Seen in *Security Wire Digest* ... seems to me it's trading the devil you know for the devil you ... know. Is WinXP really any more secure than WinNT/2K? Now if they banned the use of Outlook, that might be a step forward...

BTW, students have to pay for a copy of WinXP. Maybe this is a fundraising effort by Microsoft... put out products that are so vulnerable that users have to spend more money to buy a less vulnerable version. "I'm sorry ma'am, but the wheels frequently fall off the 1998 model cars. We have no intention of fixing the problem. Would you like to buy a 2002 model for \$20,000? By the way, you'll also need to build a new garage on your house to park it in, and a new driver's license, because the old ones aren't compatible."

***UNIVERSITY BANS WINDOWS NT/2000**

Citing security reasons, the University of California at Santa Barbara (UCSB) has banned the use of Microsoft Windows NT/2000 on its residential network, ResNet. In a posting on the ResNet site, UCSB officials blame the OSes for "hundreds of major problems on UCSB's residential network during the 2001-2 academic year," including exploited vulnerabilities, denial-of-service attacks, port scanning, and infections by Code Red and

Nimda. UCSB recommends that ResNet users switch to Windows XP Home.

<http://www.resnet.ucsb.edu/information/win2k.html>

✶ Outlook knows best! ... (Re: Kabay, [RISKS-22.30](#))

Jim Bauman <JBauman@safety-kleen.com>

Wed, 16 Oct 2002 09:42:50 -0500

I showed my boss the piece that M.E. Kabay submitted regarding Lookout, er,

I mean Outlook, always forcing the primary over the secondary address.

She's had the same experience using it at home. At work, we've been happily

using Lotus Notes for our mail client for many years. In the near future,

the powers that be will be switching us to Outlook. I can't wait!

✶ Microsoft Skins a Knee on the Astroturf

"Monty Solomon" <monty@roscom.com>

Tue, 15 Oct 2002 18:03:12 -0400

A grass-roots campaign orchestrated by a PR department is commonly called

"astroturf." What shall we call Microsoft's embarrassing sally at Apple's

successful "Switchers" campaign? Let's consider "paid testimonial." ...

No one expects Apple's ads to swing much market share, but perhaps Microsoft

was feeling their sting. On Monday the company posted a Web page, "Confessions of a Mac to PC convert," supposedly written by a young woman who had switched from Apple to Windows XP. Her name was not given. Her picture, as Slashdot posters quickly discovered, was a stock image available for purchase from Getty's Photodisc. (Why the agency did not use an image from the competing Corbis service, owned by Bill Gates, is another mystery.)

<http://newsletter.mediaunspun.com/index000021694.cfm#a100869>

⚡ Bogus Yahoo e-mail picks up credit-card numbers

Tom Van Vleck <thvv@multicians.org>

Fri, 18 Oct 2002 12:18:01 -0400

Yahoo Inc. said on 17 Oct 2002 that some of its customers had been tricked into giving their credit-card numbers to an unaffiliated third party that had posed as Yahoo in a mass e-mail. [Source: Reuters, Yahoo, 17 Oct 2002]

[http://story.news.yahoo.com/news
?tmpl=story&ncid=582&e=2&cid=582&u=/nm/20021018/wr_nm/
tech_yahoo_fraud_dc](http://story.news.yahoo.com/news?tmpl=story&ncid=582&e=2&cid=582&u=/nm/20021018/wr_nm/tech_yahoo_fraud_dc)

⚡ A new twist to Bugbear

Paul Edwards <paule@unimelb.edu.au>

Wed, 16 Oct 2002 10:15:40 +1000

I have just received a Bugbear-initiated e-mail message. What made this one different was that the body of the message contained a fragment of another e-mail message that stated a username and password for an Australian event ticket seller's e-commerce site. I set up an account on said site to see how it worked; it appears to automatically recall credit-card details upon login, as well as showing the usual personal details (address, phone number, email address, etc). There's not even an address to give the Web folks feedback.

RISKS? At least three, as I make it:

- * Sending the two authorizing IDs in the one message
- * Sending them cleartext
- * Not requiring manual entry of credit-card details per transaction

Paul Edwards, Research Support Officer, Advanced Research Computing
The University of Melbourne 3010 AUSTRALIA t: +61 3 8344 8884

[Note added 18 Oct 2002:

Just to follow up to my original posting, I finally managed to speak to someone by phone about the problem. They now appear to have removed the automatic link to credit-card details, and some (although not all) of the personal details. PE]

⚡ How we run elections in the UK

Richard Pennington <richardhelen.pennington@virgin.net>

Sat, 19 Oct 2002 16:43:55 +0000

I have been following, with a mixture of amusement and alarm, the correspondence about elections ever since Florida.

In the UK, we have a separate ballot paper for each issue at stake (perhaps we're not as democratic as the USA - there is usually just one at a time), and we use a manual count. The counters are usually "volunteered" from the class of people most likely to be able to count large numbers of pieces of paper quickly and accurately - bank cashiers.

The count proceeds in two stages: separating the votes between the various candidates, and then counting the individual piles, grouping them by elastic band into packets of 500 or 100. Dubious cases are taken out and argued over separately. The counts are scrutinised by representatives of the various political parties and others involved. A partial recount can be done very quickly by counting the number of packets in each candidate's pile (e.g. a winning count of 25,000 votes is counted by counting the 50 packets of 500 votes each), while a full recount involves recounting the number of votes in each packet (not a very long job, but necessary only if the result is close). Any candidate can claim a recount, either if there is doubt about who has won, or if there is doubt about whether a candidate has obtained enough votes to keep his deposit.

Every general election, there is an informal competition between

the various constituencies to see which can declare their result first (the declaration including a statement of the numbers of votes for each candidate, hence requiring a complete count). With an electorate averaging about 80,000 per constituency, the time to first declaration is usually just over one hour after the ballot closes.

At a general election, the result is usually clear enough for the loser at national level to concede victory before the following dawn, and the removal trucks (should they be required) move into Downing Street the day after the election (in the UK, the result is, usually, effective immediately).

The system is low-tech, but quick, reasonably efficient, recountable, and verifiable.

However, there are moves afoot to introduce electronic voting in the UK, and it was reported last week that Dr. Rebecca Mercuri visited the UK last week to voice her concerns about some of the proposed voting methods. I sincerely hope that the UK authorities will respect her knowledge and listen to her concerns.

Dr. Richard Pennington, Camberley, Surrey, UK

⚡ Re: Risks of automatic Windows updates, and HIPAA legality ([R-22.29](#))

Chuck Karish <karish@well.com>

Sun, 13 Oct 2002 09:48:49 -0700

Is Microsoft's End User License Agreement for Windows 2000 Service

Pack 3 insidious or just sloppily worded? It's possible to read it

as being meant primarily to ask for permission to execute certain tasks that the user is about to initiate: the tasks that constitute

the OS upgrade. There's a big problem, though, in that the EULA doesn't spell out that the permission being asked for is limited to

an immediate response to a specific user request.

* If you choose to utilize the update features within the OS Product or OS

Components, it is necessary to use certain computer system, hardware, and

software information to implement the features. By using these features,

you explicitly authorize Microsoft or its designated agent to access and

utilize the necessary information for updating purposes.

Microsoft may

use this information solely to improve our products or to provide

customized services or technologies to you. Microsoft may disclose this

information to others, but not in a form that personally identifies you.

* The OS Product or OS Components contain components that enable and

facilitate the use of certain Internet-based services. You acknowledge

and agree that Microsoft may automatically check the version of the OS

Product and/or its components that you are utilizing and may provide

upgrades or fixes to the OS Product that will be automatically downloaded

to your computer.

⚡ Re: Risks of automatic Windows updates, and HIPAA legality ([R-22.29](#))

<Greg Searle>

Wed, 09 Oct 2002 17:03:38 -0400

One solution is simply to turn the automatic update off. I have had a Windows 2000 system that periodically and mysteriously rebooted itself in the middle of the night. Turning this automatic update "feature" off solved the problem.

[greg_searle(at)hotmail(dot)com]

⚡ Re: Risks of automatic Windows updates, and HIPAA legality ([R-22.29](#))

Douglas Siebert <dsiebert@excisethis.khamsin.net>

Wed, 9 Oct 2002 20:34:53 +0000 (UTC)

Well, it does say "recording electrodes", which sounds to me like there's no output voltage. Unless there's a need to send a small voltage pulse out to cause a response for certain things being recorded, of course.

However, if it did control voltages, and those voltages had a range high enough to cause damage to the patient, you are correct there's a

big risk

here. Whether that's from MS having an OS that might update itself during surgery, or a hospital dumb enough to put something that could be harmful to the patient on the Internet where MS updates are only one of a number of bad things that can happen to it, I'm not sure.

✉ Re: Pac*Bell menu (Stringer-Calvert, [RISKS-22.30](#))

Crispin Cowan <crispin@wirex.com>

Tue, 15 Oct 2002 20:40:19 -0700

Seems perfectly sane to me, if you allow for modular composition.

Consider software functions. You make them general, so that they can be called from multiple contexts. From some contexts, some parameter arguments will never occur.

Now consider that the phone menus are functions

Given the sad state of software engineering, and the generally accepted view that modularity is good for software quality, I'm not particularly troubled that the phone people didn't bother to special-case this.

Crispin Cowan, Chief Scientist, WireX

<http://wirex.com/>

[~crispin/](#)

Security Hardened Linux Distribution:

<http://immunix.org>

✉ Re: Hazards of online translation and plagiarism (Mannes,

[RISKS-22.30](#)

Bob Schuchman <schuchmanr@ieee.org>

Tue, 15 Oct 2002 16:25:53 -0700

Anyone who called this story the result of an online translation and plagiarism problem hasn't read the facts at <http://www.pinoylife.com/article.php?sid=88> . An inexperienced student journalist didn't realize that pinoylife.com is an "insider" Filipino-American site with it's tongue in it's cheek. She might not even know what the tongue in the cheek meant. How she found the site is anybody's guess, but don't they have a proofreader or at least an editor at the **Daily Evergreen**?

What about the risk of telling a story without presenting all the facts and giving it a loaded title?

✶ Re: Weak encryption kills wolves (Fredriksson, [RISKS-22.29](#))

"Phil Smith III" <phs3@akphs.com>

Sun, 20 Oct 2002 23:13:53 -0400

One solution to the hunters using the wolf-tracking devices for hunting would be to deploy a large number of bogus trackers (assuming they're inexpensive enough). Perhaps a number of sheep could be equipped and deployed for this purpose, with the added benefit of providing food to help the struggling wolf population. They would, of course, also be

sheep in
wolves' clothing, so to speak...

...phsiii (smiling, um, sheepishly) [Watch out for ewe
turns. PGN]

✶ Peter L. Bernstein, Against the Gods: The Remarkable Story of Risk

"Peter G. Neumann" <neumann@csl.sri.com>
Mon, 21 Oct 2002 13:45:14 PDT

I finally caught up with a fascinating analysis of the history of risk management over the previous millennium. Although the book is somewhat slanted toward the financial world, it nevertheless has an incisive and yet broadly quasi-mathematical thoughtful perspective on risk management, and could be of interest to you. However, you might browse before you buy. It is not a typical page-turner, and is probably better digested slowly.

Peter L. Bernstein
Against the Gods: The Remarkable Story of Risk
John Wiley & Sons, New York
1996
ISBN 0-471-29563-9

The inside cover has this sentence:

This book chronicles the remarkable intellectual adventure that liberated humanity from oracles and soothsayers by means of the powerful tools of risk management that are available to us today.

[Thanks to David Huestis for lending me this book.]

★ REVIEW: "Hacking Exposed", Stuart McClure/Joel Scambray/ George Kurtz

Rob Slade <rslade@sprint.ca>
Thu, 10 Oct 2002 10:19:31 -0800

BKHCKEXP.RVW 20020911

"Hacking Exposed", Stuart McClure/Joel Scambray/George Kurtz,
2001,

0-07-219381-6, U\$49.99

%A Stuart McClure stuart@hackingexposed.com

%A Joel Scambray joel@hackingexposed.com

%A George Kurtz george@hackingexposed.com

%C 300 Water Street, Whitby, Ontario L1N 9B6

%D 2001

%G 0-07-219381-6

%I McGraw-Hill Ryerson/Osborne

%O U\$49.99 905-430-5000 fax: 905-430-5020

%P 729 p. + CD-ROM

%T "Hacking Exposed: Network Security Secrets and Solutions,
3rd Ed"

Yes, I know that this book has the most sales for any security
work,
ever. And, for the life of me, I still can't figure out why.

Part one looks at gathering data for an attack. Chapter one
discusses
company information that is generally available. However, while
it
may alert some to the fact that a lot of information can be
obtained
about them, most of the material deals with facts that you
either want

to make available, or that you must make available. Some suggested countermeasures are useful, while others strain the topic, such as the protection against domain hijacking. Scanning for weaknesses and loopholes, mostly with individual tools, in this edition, is the topic of chapter two. Enumeration, or finding weak user accounts and unprotected system resources (mostly on Windows 2000) is covered in chapter three.

Part two looks at details of specific systems. Chapter four touches on Windows 9x. NT gets a fair amount of detail in chapter five, but such vital and standard topics as disabling the Administrator account and setting up auditing are barely mentioned. Windows 2000 now has its own chapter: six. Some common NetWare attacks are listed in chapter seven. UNIX has the most extensive coverage, in chapter eight, but it is hardly comprehensive.

Part three deals with network weaknesses. Most of chapter nine discusses war-dialling and dial-up, but there is a brief mention of Virtual Private Networks (VPN). Some device weaknesses (vendor specific bugs, that is) are listed in chapter ten. (There is also a very brief mention of wardriving and detecting wireless networks.) Firewalls, in chapter eleven, are primarily addressed in terms of scanning to (for identification) or through. Chapter twelve describes a few denial of service attacks. (Something has been lost in the update: a discussion of IP fragmentation attacks refers to "earlier" material on teardrop that no longer appears in the book.)

Part four looks at software. Chapter thirteen deals with remote access software in fair detail. Hijacking and backdoors are discussed

in chapter fourteen. Miscellaneous Web site bugs are reviewed in chapter fifteen. Chapter sixteen is a confusing amalgam of ActiveX design flaws, Internet Explorer implementation bugs, and random discussions of malware.

The original preface (which no longer appears in the work) stated that the book was intended for system administrators, but it did, and still does, read more like a cookbook for security breaking. The authors defend themselves against this charge in advance, and certainly "keep quiet" versus "let it all hang out" is a constant debate in security circles. However, the attack descriptions are far more detailed than the countermeasures sections, and many attacks are presented without any specific protections being mentioned. There are a number of points in the book that can be helpful in identifying specific security weaknesses. However, the book can't be comprehensive in that regard, and what it fails to do is give an overall concept of, or framework for, security on an ongoing basis. The examples given are frightening and stimulating, but the authors present them as the entire picture. In fact, even the picture as presented is not entire. A number of descriptions given in the book either do not mention, or gloss over, the fact that, for example, sniffers must be placed on a local, promiscuous, network, and session hijacking requires that the attackers somehow get "between" two systems.

On the other hand, the book is quite readable and can give you some tips. And, I wouldn't mind seeing a few sysadmins a little more scared

than they
are at the moment. As long as they don't think that this is
all you need
to do.

copyright Robert M. Slade, 2000, 2002 BKHCKEXP.RVW 20020911
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com
<http://victoria.tc.ca/techrev> or <http://sun.soci.niu.edu/~rslade>

REVIEW: "Have You Locked the Castle Gate", Brian Shea

Rob Slade <rslade@sprint.ca>
Mon, 21 Oct 2002 08:17:56 -0800

BKHYLTCG.RVW 20020825

"Have You Locked the Castle Gate", Brian Shea, 2002, 0-201-71955-X,
U\$19.99/C\$31.99
%A Brian Shea
%C P.O. Box 520, 26 Prince Andrew Place, Don Mills, Ontario
M3C 2T8
%D 2002
%G 0-201-71955-X
%I Addison-Wesley Publishing Co.
%O U\$19.99/C\$31.99 416-447-5101 fax: 416-443-0948
%P 193 p.
%T "Have You Locked the Castle Gate: Home and Small Business
Security"

Chapter one is entitled "Assessing Risk." It deals with the
basic concepts,
but in a somewhat confused manner, and sometimes stresses or
sensationalizes
minor points. A grab bag of security concepts drifts into
Windows specifics

in chapter two. The author has said that he will be concentrating on Windows, since it is the most widely used system for home computers, but the material tells only *how* to, for example, set up groups, and not what groups are used for in terms of security. Chapter three is more of the same: more miscellany, and more Windows. The discussion of servers, in chapter four, is almost entirely devoted to Windows, and is weak on security concepts and technologies such as firewalls. There is a set of vague ideas about the Internet in chapter five. Chapter six, on email security, has some good suggestions, but a number of gaps. Web security is a questionable checklist of browser settings, almost entirely for Internet Explorer, in chapter seven. "Defending Against Hackers," in chapter eight, sounds like it should be important, but it is hard to find any point. Chapter nine, on viruses, starts with a surprisingly good set of definitions (recognizably from "Robert Slade's Guide to Computer Viruses") but quickly deteriorates into errors (the Internet Worm was *not* an accident), and poor suggestions (it does not make an awful lot of sense to talk about "boot disks" for scanning Windows systems without getting into a lot of detail).

I am all in favour of having a relatively simple and straightforward guide to security for home and small business users. But Jeff Crume already did "Inside Internet Security" (cf. BKININSC.RVW), and did a much better job.

copyright Robert M. Slade, 2002 BKHYLTCG.RVW 20020825
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca

p1@canada.com

[http://victoria.tc.ca/techrev
~rslade](http://victoria.tc.ca/techrev/~rslade)

or

<http://sun.soci.niu.edu/>



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 32

Weds 23 October 2002

Contents

- [Hacker attack targets root servers](#)
[NewsScan](#)
- [Memo reveals FBI national security wiretap violations](#)
[Marc Rotenberg](#)
- [Math in the cockpit: yet another units conversion risk](#)
[George N. White III](#)
- [Navy searching for missing computers](#)
[Bradley Wood](#)
- [FDA approves implantable ID chip](#)
[NewsScan](#)
- [Family receives enormous deposit in error](#)
[Ulf Lindqvist](#)
- [Bugbear hugs?](#)
[Justin Macfarlane](#)
- [Privacy Journal Ranking of States](#)
[Robert Ellis Smith](#)
- [IE flaws leave systems vulnerable](#)
[Monty Solomon](#)
- [Re: The high risk of low security: element 118](#)
[Mike Hogsett](#)

[Stephen Poley](#)

● [Re: UCSD bans WinNT/2K -- NO, it is UCSB](#)

[Tom Perrine](#)

● [Re: UCSB bans WinNT/2K -- will it do any good](#)

[Alistair McDonald](#)

● [Re: password complexity ...](#)

[Jeremy Ardley](#)

[Martyn Thomas](#)

[Merlyn Kline](#)

[Miro Jurisic](#)

[Jordin Kare](#)

● [REVIEW: "Secure XML", Donald E. Eastlake/Kitty Niles](#)

[Rob Slade](#)

● [REVIEW: "Hack Proofing Your Identity in the Information Age", Teri Bidwell](#)

[Rob Slade](#)

● [Info on RISKS \(comp.risks\)](#)

🔥 Hacker attack targets root servers

"NewsScan" <newsscan@newsscan.com>

Wed, 23 Oct 2002 08:58:30 -0700

A powerful denial-of-service attack briefly crippled nine of the 13 Internet

"root" servers, but traffic routing was able to continue unimpeded, said

ICANN VP Louis Touton: "As best we can tell, no user noticed and the attack

was dealt with and life goes on." One government official described

Monday's attack as the most sophisticated and large-scale assault on these

root servers to date. The attack, which began around 4:45 p.m. EDT on

Monday, blasted the servers with 30 to 40 times the normal amount of

messages, rendering seven computers unable to respond to

legitimate Internet traffic. Two others failed intermittently during the attack. The Internet theoretically can run with just one operational root server, but response times would be very slow. [AP 23 Oct 2002; NewsScan Daily, 23 October 2002]

<http://apnews.excite.com/article/20021023/D7MR8PT00.html>

✶ Memo reveals FBI national security wiretap violations

Marc Rotenberg <rotenberg@epic.org>

Thu, 17 Oct 2002 15:47:06 -0400

[Excerpted from EPIC Alert 9.19. PGN]

A recently released FBI memo provides the latest evidence that the Bureau has frequently overstepped its legal bounds when conducting intrusive national security surveillance. The document, which was written in April 2000 and originally classified as "secret," reveals that FBI agents illegally videotaped suspects, intercepted e-mail without court permission, recorded the wrong phone conversations, and conducted "unauthorized searches." The incidents detailed in the memo involved cases requiring warrants under the Foreign Intelligence Surveillance Act (FISA).

The declassified document was obtained by Rep. William Delahunt (D-MA), with the assistance of EPIC. The existence of the memo was first revealed in an FBI document obtained by EPIC earlier this year through its Freedom of

Information Act lawsuit for information concerning the Bureau's controversial Carnivore Internet surveillance system (see EPIC Alert 9.11).

That earlier disclosure, which showed that an anti-terrorism investigation involving Osama bin Laden was hampered by technical flaws in the Carnivore system, alluded to a separate document discussing other "FISA mistakes." EPIC worked with Rep. Delahunt's office to seek disclosure of the "mistakes" memo.

The latest disclosure comes as the Foreign Intelligence Surveillance Court of Review (FISCR), in its first proceeding since being created in 1978, is considering the legality of new Justice Department surveillance rules. DOJ has asked the FISCR to overturn a decision of the Foreign Intelligence Surveillance Court, which in May unanimously rejected the government's bid for expanded powers. In its decision, the intelligence court documented abuses of "national security" warrants by both the Bush and Clinton Administrations, including serious errors in approximately 75 applications for foreign intelligence surveillance (see EPIC Alert 9.16).

The newly disclosed "mistakes" memo reveals errors that extend beyond those detailed by the surveillance court in May, which concerned FBI misrepresentations in applications for surveillance warrants. The new "mistakes" involve the manner in which surveillance activities were actually conducted, a potentially more serious issue as the incidents appear to involve violations of both FISA and the Fourth Amendment.

The FBI "FISA mistakes" memo is available at:

<http://www.epic.org/privacy/terrorism/fisa/FISA-mistakes.pdf>

Background information (including selected documents) on EPIC's Carnivore FOIA litigation is available at:

<http://www.epic.org/privacy/carnivore/>

Background information on FISA is available at:

<http://www.epic.org/privacy/terrorism/fisa/>

✶ Math in the cockpit: yet another units conversion risk

"George N. White III" <aa056@chebucto.ca>

Tue, 22 Oct 2002 21:44:25 -0300 (ADT)

An article by Mark Bowden in the November, 2002, Atlantic Monthly describes the process of delivering smart bombs as practiced in Afghanistan. Air Force pilots working with Army "forward air controllers" (FAC) sometimes drop laser guided precision bombs through cloud cover using guidance from a laser operated by the FAC. The Army uses different coordinate systems for position and elevation from that of the Air Force. Apparently the Air Force system does not provide for coordinate conversion, so the "weapons system officer" (WSO) must make manual calculations to convert coordinates, often under intense pressure, including watching for a ground-to-air missile launch. After one such episode, Bowden quotes one WSO as saying, "The recruiter said there would be no math in the cockpit". In fact, the ability to do simple math under pressure has always been an important cockpit skill.

Years ago, pilots carried circular slide rules to perform fuel and distance calculations. The WSO quoted in the article used a calculator in his watch.

The risks associated with a system that requires manual coordinate conversion are clear -- many examples have appeared in this forum. We may never know how many people died in Afghanistan as a result of errors in manual coordinate conversions, either as direct casualties from a misdirected bomb or as a result of enemy action that a properly directed bomb would have prevented.

George N. White III <aa056@chebucto.ns.ca>
Head of St. Margarets Bay, Nova Scotia, Canada

🚨 Navy searching for missing computers

"Bradley Wood" <Bradley.Wood@sri.com>
Tue, 22 Oct 2002 10:17:50 -0600

At least 595 laptops and desktops belonging to the Navy's Pacific Command in Hawaii were reported as potentially lost or compromised, according to a July 2002 inventory of onboard units performed by the Naval Audit Service. The report identifies failures and breakdowns in the Navy's largely manual system for tracking sensitive equipment deployed aboard Navy ships and submarines. However, the number was reduced to 187 by mid-October, after further checking. Shore-based units are now being surveyed, and a new inventory control system is being developed. In August, two top-

secret

laptops disappeared from a Sensitive Compartmented Information Facility (SCIF) run by the U.S. Central Command at MacDill Air Force Base in Tampa, Fla. This was detected as part of an attempt to find out how plans for an invasion of Iraq had leaked to the media. [Various similar cases were noted involving the U.S. Departments of State, Energy, and Justice, and the FBI.]

[Source: Dan Verton, 21 Oct 2002, *Computerworld*; PGN-ed]
www.computerworld.com/securitytopics/security/story/0,10801,75295,00.html

✶ FDA approves implantable ID chip

"NewsScan" <newsscan@newsscan.com>

Wed, 23 Oct 2002 08:58:30 -0700

In a surprise move, the Food and Drug Administration okayed the use of implantable ID chips in humans, providing they are used for "security, financial and personal identification or safety applications." The FDA has still not ruled on whether the VeriChip, made by Applied Digital Solutions, can be used for medical purposes, however. The company has promoted the device in the U.S. for its ability to provide detailed medical history data in cases where the patient is unable to communicate with emergency room personnel. Applied Digital president Scott Silverman says he's happy with the FDA's decision: "We'll now go into high gear with our sales, marketing

and distribution plans in the U.S.," adding that the company will focus on the security and ID aspects of the chip, at least for the time being.

Meanwhile, Leslie Jacobs, whose family volunteered to "get chipped" last May, says she's still hoping the FDA will approve the VeriChip for medical use. Both her husband and son have ongoing health problems. [Wired.com 23

Oct 2002; NewsScan Daily, 23 October 2002]

<http://www.wired.com/news/politics/0,1283,55952,00.html>

✶ Family receives enormous deposit in error

Ulf Lindqvist <ulf@sdl.sri.com>

Tue, 22 Oct 2002 16:53:33 -0700 (PDT)

We have heard of bogus deposits before, but this one is unusually high.

The Swedish local newspaper *Tidningen Angermanland* (www.tidningen.to) reports that a "human error" caused an amount of more than 92,700,000,000 SEK (roughly \$10 billion, or 10 milliard Euro if you will) to be deposited into the bank account of a family, instead of the normal 950 SEK per child per month that all families in Sweden receive from the government. The bank spokesperson said that payments were processed manually because of a backlog caused by other problems, and would not elaborate on the actual cause, citing security concerns. After less than a day, the payment was reversed, and the family were not allowed to keep the 15 million SEK of

interest that
had accrued on their account during this time.

✶ Bugbear hugs?

"Justin Macfarlane" <Justin.Macfarlane@lafferty.com>
Tue, 22 Oct 2002 10:44:19 +0100

The recent Bugbear epidemic recently had pleasant repercussions for a colleague. An e-mail they had sent to an external business, which later became infected with the virus, was chosen for mass circulation. It ended up in many people's inboxes, one of whom turned out to be an old university friend. They had lost contact over the years, and thanks to the virus, now they're back in touch.

✶ Privacy Journal Ranking of States

"Robert Ellis Smith" <ellis84@rcn.com>
Tue, 22 Oct 2002 10:25:23 -0400

PRIVACY JOURNAL ISSUES RANKING OF STATES IN PRIVACY

California ranks highest in protecting its citizens against invasions of privacy, according to a ranking issued by Privacy Journal, the nation's leading publication on privacy.

California finished at the top because its legislature passed a

raft of new protections in the last two years; also, its courts and its constitution provide the strongest privacy protection in the nation.

In 1999, when the Providence, R.I.-based monthly newsletter announced its first ranking of the states, California and Minnesota tied for first. This year, after Privacy Journal considered laws and practices since 1999, California finished first and Minnesota finished second, both with numerical rankings 33 percent higher than the next ranked state.

The top ten states, according to the Providence R.I.-based monthly newsletter, are, in alphabetical order: California, Connecticut, Florida, Hawaii, Illinois, Massachusetts, Minnesota, New York, Washington, and Wisconsin. There was little change among the top ten states from Privacy Journal's original ranking of the states, in 1999. California and Minnesota tied in 1999. California, Minnesota, and Hawaii - alone among the states - have state offices assigned to protect personal privacy.

The ranking is based on the 2002 edition of Privacy Journal's "Compilation of State and Federal Privacy Laws," a 106-page reference book available for \$35 from Privacy Journal, PO Box 28577, Providence RI 02908, 401/274-7861, fax 401/274-4747, orders@privacyjournal.net, www.privacyjournal.net.

Privacy Journal rates the states on several factors, including whether they protect privacy in their constitutions, have laws protecting financial, medical, library, and government files, and have fair credit

reporting laws
stronger than the federal law. Points are added when the highest
court in
the state has a strong record on privacy and deducted for anti-
privacy
actions by state agencies or the state legislature.

Contact: Robert Ellis Smith, 401/274-7861
orders@privacyjournal.net
<http://www.privacyjournal.net>

[See the Web site for further details. PGN, who is now on the
Advisory Council of the California Office of Privacy
Protection...]

IE flaws leave systems vulnerable

"Monty Solomon" <monty@roscom.com>
Tue, 22 Oct 2002 16:27:18 -0400

By Robert Lemos, Staff Writer, CNET News.com, 22 Oct 2002

An Israeli Web-application company has warned users of Internet
Explorer
that nine related security flaws in the program could be used by
malicious
hackers to gain access to a victim's computer files. GreyMagic
Software
said Tuesday that the vulnerabilities--eight of which it deemed
critical --
could be exploited using a specially coded Web page that would
run malicious
programs on a victim's computer if the victim visited the
page. ...

<http://news.com.com/2100-1001-962966.html>

⚡ Re: The high risk of low security: element 118 ([RISKS-22.31](#))

Mike Hogsett <hogsett@csl.sri.com>

Mon, 21 Oct 2002 16:25:47 -0700

> [What to name the would-be new element?
> Phonium? Phakium? Phorgium? Phudgium? PGN]

Itaintium?

[PGN notes this includes a nice pun: It-ain't-ium vs I-taint-ium]

Unscrupulum?

⚡ Re: The high risk of low security: element 118 ([RISKS-22.31](#))

Stephen Poley <sbpoley@xs4all.nl>

Tue, 22 Oct 2002 16:56:04 +0200

Given elements 102 Nobelium and 101 Mendeleevium, 118 would obviously be

Nobelievium

[Sent to RISKS via Mark Brader... apparently from an UNMODERATED

comp.risks pipeline over which I have no control! PGN]

⚡ Re: UCSD bans WinNT/2K -- NO, it is UCSB (Epstein, [RISKS-22.31](#))

Tom Perrine <tep@sdsc.edu>

Tue, 22 Oct 2002 09:21:43 -0700

There's an error in the subject line of Jeremy Epstein's message. It is UCS*B* that is banning NT/2000, not UCS*D* (where I am). However, it is correct in the story itself.

> Citing security reasons, the University of California at Santa Barbara
> (UCSB) has banned the use of Microsoft Windows NT/2000 on its residential
> network, ResNet. ...

✉ Re: UCSB bans WinNT/2K -- will it do any good

"Alistair McDonald" <alistair@inrevo.com>
Tue, 22 Oct 2002 12:52:20 +0100 (BST)

An interesting opposite to this story is a thread on the uk.comp.os.linux, where King's College (London University) bans the connection of Unix and Linux systems to their network.

The thread is archived here:

<http://groups.google.com/groups?dq=&hl=en&lr=&ie=UTF-8&threadm=7d532ada.0209180542.6503efb6%40posting.google.com&rnum=1&prev=/groups%3Fq%3Dg:th1127390037d%26dq%3D%26hl%3Den%26lr%3D%26ie%3DUTF-8%26selm%3D7d532ada.0209180542.6503efb6%2540posting.google.com>

Now, a badly administered box is a risk to everyone, no matter the OS, but this seems to be a trifle heavy-handed.

Alistair McDonald, InRevo Ltd.

Land: +44 1344 642 521 Mobile: +44 7812 829 020 <http://www.>

inrevo.com

✶ Re: password complexity ... (Arnold, [RISKS-22.31](#))

Jeremy Ardley <jeremy@electrosilk.net>

Tue, 22 Oct 2002 09:28:28 +0800

Seth Arnold <sarnold@wirex.com> wrote about the security implications of putting 10 electronic numerals onto only 5 buttons. This is not a bright idea from the electronic age, but simply a rehash of traditional locksmithing practice.

Many combination locks may have 100 or more marks on the dial, but physically have far less. So for instance, selecting 57 on the dial could work equally as well if you chose any number from 55 to 60.

I quote from a published project by Neil Fraser on how to crack cheap 60 mark 3 wheel combination locks using custom built machinery:
<http://neil.fraser.name/hardware/locraker/>

"Its strategy is essentially the brute-force approach of trying all combinations until the lock opens; however it uses several short cuts. A standard combination lock does not have 60 possible divisions (as its dial might suggest), but rather more like 15. To be thorough, the Locraker assumes 20 divisions. Thus the number of possible combinations is 20*20*20 or 8000. Another shortcut is that it doesn't have to dial in all three numbers separately for each try. Instead, it can dial in the

first two

numbers, then try all the possible third numbers in one pass by continually jerking the clasp as it spins the dial around once. The lock

doesn't know it is being repeatedly polled. This reduces the number of

passes to 20×20 or 400. Finally, the average lock will open after half the

combinations have been tried, so the expected number of passes would be

200. At six and a half passes per minute, it can open a lock in about half an hour."

✶ Re: password complexity ... (Arnold, [RISKS-22.31](#))

"Martyn Thomas" <martyn@thomas-associates.co.uk>

Tue, 22 Oct 2002 09:28:28 +0800

My digital lock has ten buttons, one per digit, and has a five digit code.

An examination of the mechanism shows that it doesn't matter in what order the digits are entered ...

I have never met a computer password system with that particular weakness.

Martyn Thomas, Holly Lawn, Prospect Place, Bath BA2 4QP 01225 335649

✶ Re: password complexity ... (Arnold, [RISKS-22.31](#))

"Merlyn Kline" <merlyn@zyweb.com>

Tue, 22 Oct 2002 09:56:15 +0100

> Date: Sat, 19 Oct 2002 17:15:15 -0700
> From: Seth Arnold <sarnold@wirex.com>
> Subject: Password complexity -- not just for computers anymore
>
> The outside key-code on my building has five buttons but ten
digits -- two
> digits per button. This allows for 10^n different
"combinations" as humans
> must remember it, but 5^n different combinations as the door
remembers it.

Either 5^n combinations provides adequate security or it does
not. If it
does not, then the system is flawed regardless of key labelling.
If, OTOH,
it *does* provide adequate security then you could report the
key labelling
as follows:

"The outside key-code on my building has five buttons but ten
digits -- two
digits per button. This allows for 5^n different combinations,
each with 2^n
mnemonic representations thus reducing the number of false
negatives and the
need to re-issue codes to those who have forgotten theirs."

Of course if people are allowed to choose their own codes then
there is an
increased chance of two people choosing the same code. However
if this is a
problem for the implementation of this particular system then it
needs to be
managed anyway.

Merlyn Kline

⚡ Re: password complexity ... (Arnold, [RISKS-22.31](#))

Miro Jurisic <macdev@meero.org>

Tue, 22 Oct 2002 09:19:22 -0400

I believe the intent here is to allow you to use the same combo on two different doors, one using a 3x4 grid, one using five buttons. MIT uses this in public computer clusters, where all the older combo pads are 3x4 and the newer ones are 1x5, yet the same combo can be used on all of them.

⚡ Re: password complexity ... (Arnold, [RISKS-22.31](#))

Jordin Kare <jtkare@attglobal.net>

Tue, 22 Oct 2002 02:55:29 -0700

This one isn't a mistake, it's quite deliberate, and (arguably) sensible.

The intent is to allow people to use any number they want as a combination -- birthdate, phone number, building-number-plus-3, etc. If only digits 1-5 were shown, then most such easy-to-recall numbers wouldn't work, and the combination would have to be remembered like a random-character password string. Code locks on luxury car doors use the same arrangement, for the same reason, and the letters on telephone keys serve an equivalent function. (Originally for translating named exchanges to numbers -- MOhawk 4, BUTterfield 8 -- but now mostly for advertising; it's easier to

remember
I-FLY-SWA than 435-9792).

Of course, encouraging people to use an easily-recalled number does lower the security level, but 5-button locks are not generally intended for strong security. (On one occasion, I opened one with the second "random" combination I tried, much to the bemusement of the secretary whose office it was supposed to be protecting.)

Jordin Kare, 222 Canyon Lakes Pl., San Ramon, CA 94583

🔥 REVIEW: "Secure XML", Donald E. Eastlake/Kitty Niles

Rob Slade <rslade@sprint.ca>
Tue, 22 Oct 2002 07:15:08 -0800

BKSECXML.RVW 20020831

"Secure XML", Donald E. Eastlake/Kitty Niles, 2003, 0-201-75605-6,

U\$44.99/C\$69.99

%A Donald E. Eastlake III

%A Kitty Niles

%C P.O. Box 520, 26 Prince Andrew Place, Don Mills, Ontario
M3C 2T8

%D 2003

%G 0-201-75605-6

%I Addison-Wesley Publishing Co.

%O U\$44.99/C\$69.99 416-447-5101 fax: 416-443-0948

%P 532 p.

%T "Secure XML: The New Syntax for Signatures and Encryption"

Part one is introductory material. Chapter one is about XML (eXtensible Markup Language), but is not very clear, especially in

regard to the relationship between XML, SGML (Standard Generalized Markup Language), and HTML (HyperText Markup Language). Security concepts do not play a big part. The tutorial on cryptography, in chapter two, is very simplistic, uses obtuse language, and is much harder on the reader than is really necessary.

Part two deals with the basics of XML. Chapters three through eight present some of the syntax and structure of XML documents, DTDs (Document Type Definitions), Schemas (particularly unclear), XPath, XPointer, and SOAP. That is about all they provide: the material is not helpful in explaining uses, or how the parts fit into a framework or package.

Part three covers canonicalization and authentication. Canonicalization is important to authentication, as chapter nine points out, because it allows us to eliminate meaningless differences between essentially the same file, as when different file systems use varying newline characters or sequences. Ordinarily, such differences would result in differences in hash code results, and therefore a false failure of authentication. Chapter ten outlines signature syntax, while eleven talks very briefly about the XMLDSIG standard for digital signatures, and twelve reviews the European Telecommunications Standards Institute's (ETSI) somewhat more advanced signatures.

Part four looks at keying, with the KeyInfo element in chapter thirteen, and XKMS key management in fourteen. Chapter fifteen, on the proposed XMLENC standard, and sixteen, containing some discussion of combinations of encryption and signatures, make up part five. Part

six, entitled "Algorithms," reviews algorithm specification, in chapter seventeen; available algorithms, in eighteen; and related non-cryptographic algorithms, in nineteen.

The writing is turgid, almost deliberately dense, and fails to provide necessary tutorial details. Those who are well familiar with XML will find some particulars regarding the specific encryption documents, but few others will find the work useful.

copyright Robert M. Slade, 2002 BKSECXML.RVW 20020831
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

<http://victoria.tc.ca/techrev/~rslade> or <http://sun.soci.niu.edu/~rslade>

⚡ REVIEW: "Hack Proofing Your Identity in the Information Age", Teri Bidwell

Rob Slade <rslade@sprint.ca>
Wed, 23 Oct 2002 07:14:25 -0800

BKHPYIIA.RVW 20020826

"Hack Proofing Your Identity in the Information Age", Teri Bidwell,

2002, 1-931836-51-5, U\$29.95/C\$46.95

%A Teri Bidwell

%C 800 Hingham Street, Rockland, MA 02370

%D 2002

%G 1-931836-51-5

%I Syngress Media, Inc.

%O U\$29.95/C\$46.95 781-681-5151 fax: 781-681-3585 www.syngress.com

%P 370 p.

%T "Hack Proofing Your Identity in the Information Age"

Chapter one does say a bit about what identity theft is, and suggests some basic protections against it. The rest of the book, however, seems to be just another attempt to provide an "easy" security book for home users. And it doesn't do it very well.

Chapter two is a miscellaneous grab bag. It recommends keeping all your files in a standard place (bad), has some nice content on cleaning up temporary files (good), suggests novice users change the Registry (dangerous), promotes the use of a power on password (good), has rotten material on viruses and trojans (conflicting definitions on facing pages as well as a confusion of adware and spyware, although it does get a point for mentioning F-Prot), insists users install all patches (possibly bad), outlines how to set up multiple accounts (good), and has some decent advice on choosing passwords (also good). There is a range of information on e-mail security in chapter three, although the details are questionable. The "man-in-the-middle" attack is described as TCP hijacking and is said to be foiled by cryptography, when, in fact, it is usually an attack on cryptography. There is good advice on scams. Web security, in chapter four, is heavy on cookies and e-commerce, and light on many more serious issues. Chapter five is generic Internet connection information. It defines a sniffer correctly once but elsewhere as a keylogger, and oversimplifies firewalls. Random topics loosely related by being popular

with kids make up chapter six. Chapter seven does return to the topic of identity theft and discusses what to do if it occurs. Some of the advice is helpful (particularly if you live in the US), but most is vague common sense. There is a repeat of the material (with slightly more detail) on firewalls and browser settings, in chapter eight.

There is little here that is specific to the titular topic. As for a general security text, Jeff Crume (cf. BKININSC.RVW) as well as Cronkhite and McCullough (cf. BKACCDEN.RVW) have already done it better.

copyright Robert M. Slade, 2002 BKHPYIIA.RVW 20020826
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

<http://victoria.tc.ca/techrev> or <http://sun.soci.niu.edu/~rslade>



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

[ACM](#) Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 33

Friday 1 November 2002

Contents

- [Home isn't where the security is](#)
[NewsScan](#)
- [Autotote programmer hacks winning Pick Six bets](#)
[Lillie Coney](#)
- [iVotronic voting machines lose 294 early votes](#)
[Tom Adams](#)
- [Voting machines postpone the end of Brazil's daylight saving time](#)
[Nik Clayton](#)
- [Software failure informs eavesdropped phone users](#)
[Markus Kuhn](#)
- [Decimal glitch spurs hotel overbill](#)
[Fuzzy Gorilla](#)
- [Possible role of simulator scenario in AA crash](#)
[Cathy Horiuchi](#)
- [Re: Slide rules in the cockpit](#)
[Eric Remy](#)
- [FDA permits use of ID chips in humans](#)
[Roger Clarke](#)
- [REVIEW: "Managing Information Security Risks", Alberts/Dorofee](#)
[Rob Slade](#)

- [REVIEW: "EW 101: A First Course in Electronic Warfare", David Adamy](#)
[Rob Slade](#)
 - [REVIEW: "Disaster and Recovery Planning", Joseph F. Gustin](#)
[Rob Slade](#)
 - [CFP, Security and Control of IT in Society: SCITS III](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Home isn't where the security is

"NewsScan" <newsscan@newsscan.com>

Tue, 29 Oct 2002 08:44:26 -0700

Columnist Robert Lemos says the Bush administration's plan to ask home computer users to secure their systems as part of its "National Strategy to Secure Cyberspace" is a misguided effort. Citing the prevalence of users who still call tech support wondering why their computer won't turn on (because they've neglected to plug it in), Lemos says: "The experts are guilty of wrongheaded thinking in relying upon home users to shore up the nation's security. Frankly, that's somebody else's job. Home users are responsible for protecting their own important data. But it's a dangerous illusion to believe they will take better precautions after authorities ask them to upgrade their cyberdefenses." Lemos says the government instead should be focusing on persuading the ISPs "to protect cyberspace from home users. There are simple technologies for doing this. Source egress filtering -- a technique for preventing users from sending data

with a false source address, useful in denial-of-service attacks -- should be the norm.

Companies filter e-mail messages for any viruses and disallow several types of executable attachments; ISPs should do the same." Security expert Dorothy

Denning says the only question left is, who will pay? "Once you start

formalizing where we are going to put liability, the questions start coming

up about who's going to pay for it. And, almost anywhere you put it, the

costs are going to end up coming back to the users." [CNet News.com 29 Oct

2002; NewsScan Daily, 29 October 2002]

<http://news.com.com/2010-1071-963614.html?tag=lh>

[This seem like old news to long-time RISKS readers, but the fundamentally inadequate approach of relying only on users to do

something rather palliative totally ignores the rampant vulnerabilities

in the computer-communication systems provided by mass-market software

developers, ISPs, and others. It seems to reflect an abysmal lack of

understanding of or perhaps willful obliviousness to the pervasiveness

of problems associated with security and other trustworthiness issues

(reliability, survivability, etc.) by folks who should know better...

The marketplace does not solve these problems. PGN]

✶ Autotote programmer hacks winning Pick Six bets

Lillie Coney <lillie.coney@acm.org>

Fri, 01 Nov 2002 09:44:00 -0500

Autotote (a subsidiary of Scientific Games Corp in New York state) develops the software for most of the nation's off-track betting systems. One of its programmers apparently "software-engineered" the system to yield a \$3 million Pick Six payoff from the Catskill NY OTB site, to be collected by a man in Baltimore who had placed his bets by phone before the first race. The bets were somewhat unusual: picks for the first four races, and wild-card multiple bets spanning all possibilities for the remaining two races. Because of a design decision to minimize loading of the Autotote system, local OTB data on the first four sets of bets is not posted to the host network until just after the first four results were known. Apparently, a little internal engineering resulted in the first four bets being altered to name the winners of the first four legs, including 26-to-1 and 13-to-1 long shots, along with all possible combinations for the fifth and sixth races. The Baltimore man was the only person with the winning Pick-6 combination, and also had consolation combinations for picking 5 out of 6. We presume some sort of collusion. However, a spokesman for SGC said that their anomaly detection system caught this event before any payoffs occurred, after which 72 other consolation winners were then allocated proportionally larger sums. He added that he and his technical people had "considered it absolutely impossible" to hack into the system. One wag later posted a note on the SGC Internet Web site asking if he could still post a bet on those races. Incidentally, the programmer has

been fired, and
the case is under investigation. [Source: Computer programmer
fired in Pick
Six investigation, Greg Sandoval and John Scheinman, *The
Washington Post*,
1 Nov 2002, D01; PGN-ed]

[In this forum, we have been long been noting many of the
risks in
gambling systems as well as in electronic voting systems.
Even in a
system that has seemingly been carefully designed for security
and
integrity, a little bit of insider action can result in very
nasty
results. PGN]

✶ Machines lose 294 early votes

<Adams.Tom@epamail.epa.gov>
Thu, 31 Oct 2002 11:19:28 -0500

iVotronic voting machines lost 294 votes at early voting site in
Wake
County, NC due to a "glitch in the software".

Officials apparently have the names of the voters but have lost
their
virtual ballots. They are trying to contact the
voters so that they can revote. Given the times and locations
in the
article, I may be one of those voters!

<http://newsobserver.com/news/triangle/story/1876251p-1865783c.html>

✶ Voting machines postpone the end of Brazil's daylight saving time

Nik Clayton <nik@freebsd.org>
Sat, 26 Oct 2002 10:56:48 +0100

A recent revision to the timezone files used by (among other operating systems) FreeBSD highlights an unforeseen risk of electronic voting.

This year the Brazilian elections were sufficiently close that a second round of voting is required. This will take place on October 27th, which would normally be after the DST transition.

The Brazilian Constitution requires elections to start at 8am and finish at 5pm. However, Brazil's vote counting systems are computerised, and the electoral machines can not have their internal clock changed. Rather than change the constitution, or do the necessary timezone adjustments to the output of the electoral machines, Brazil's government decided to postpone the DST transition.

The diff (at <http://www.freebsd.org/cgi/cvsweb.cgi/src/share/zoneinfo/southamerica.diff?r1=1.19&r2=1.20>) has more details in the comments.

✶ Software failure informs eavesdropped phone users

Markus Kuhn <Markus.Kuhn@cl.cam.ac.uk>

Thu, 31 Oct 2002 14:28:52 +0000

The **Sueddeutsche Zeitung** in Munich reports:

Thanks to a rather absurd accident, dozens of suspected extremists and criminals obtained proof that their phones were being tapped by German security services. A few days ago, they received from their phone company 02 an invoice that listed and billed connections to a mailbox unknown to them. For instance, a man in Berlin was asked to pay phone charges of 15.35 euros for 53 connections made during 3-30 September 2002 to always the same mailbox. At the listed number, a voice informs the caller about a lack of authorization. The accident was discovered when the customer complained with his phone company.

Security sources confirmed Monday that around 50 persons, all of whose phone numbers start with +49 179, had been invoiced for eavesdropping costs. Initially, the authorities suspected a much larger number of persons, because the number of phone taps is high. According to latest informations from the telecommunication services providers, almost 20000 lines are being recorded at present in Germany. The number of lines under surveillance has increased particularly significantly since 11 September 2001.

Security services contacted 02 in Munich immediately after the accident was noticed and stopped the delivery of printed but not yet mailed invoices. Security service sources claimed that the problem was triggered by a

software update.

[Summarizing translation by M. Kuhn]

Source: Annette Ramelsberger: "Beweis auf dem Silbertablett -
Durch

Panne tauchten Abhörkosten auf Telefonrechnung auf", Sueddeutsche
Zeitung, Munich, Germany, 2002-10-31.

[http://www.sueddeutsche.de/aktuell/sz/getArticleSZ.php?
artikel=artikel4992.php](http://www.sueddeutsche.de/aktuell/sz/getArticleSZ.php?artikel=artikel4992.php)

Markus Kuhn, Computer Lab, Univ of Cambridge, GB

<http://www.cl.cam.ac.uk/~mgk25/> | __oo_0..0_oo__

[This article also noted by Martyn Thomas. In addition
Florian Liekweg, IPD Universität Karlsruhe, reported on an
article in

in *Frankfurter Rundschau*, with original German at

<http://www.heise.de/newsticker/data/jk-30.10.02-006/>

02 was formerly known as Viag Interkom. PGN]

⚡ Decimal glitch spurs hotel overbill

"Fuzzy Gorilla" <fuzzygorilla@euroseek.com>

Fri, 01 Nov 2002 17:33:06 -0500

[I have to wonder what happened to basic software testing?]

If you stayed at a Holiday Inn, Holiday Inn Express, or Crowne
Plaza hotel

and checked out between 24 Oct and 26 Oct 2002, you are likely
to have been

one of 26,000 people who were charged 100 times what they owed,
such as

\$6,500 to \$21,000 per night. A credit-processing error resulted
in the

decimal points being dropped. Most of the charges were later
reversed,

although many people discovered that their credit limits had been exhausted.

Overcharged guests will get two free nights at any of those hotels.

[Source: Article by Russ Bynum, Associated Press, 01 Nov 2002; PGN-ed]

<http://story.news.yahoo.com/news>

[?tmpl=story2&u=/ap/20021101/ap_on_re_us/guests_overcharged](http://story.news.yahoo.com/news?tmpl=story2&u=/ap/20021101/ap_on_re_us/guests_overcharged)

✶ Possible role of simulator scenario in AA crash

Cathy Horiuchi <cmhoriuc@pacbell.net>

Thu, 31 Oct 2002 14:02:28 -0800

Wall Street Journal, 31 Oct 2002, p. D10,
American Revised Training Methods in Wake of Crash

The role of simulators in predisposing pilots to particular strategies is part of the NTSB investigation into last year's crash of AA flight

587. From the article...

"Mr. Young said that until earlier this year, American flight instructors

routinely set the stage for practicing upset recoveries in simulators by

telling pilots to pretend they had just entered the wake of a preceding

jumbo jet. Then the simulator was instructed to depict a sharp roll or

steep nose-up maneuver, which typically required a fair amount of rudder

input to correct."

This resembles issues surrounding decoding any constructed "word problem"

into a "math problem". Scenario setters decided on the physical

forces --

and it seems from this report, the solution -- then programmed it into the simulator; the equivalent of a fully articulated mathematical problem. Then

they gave the pilots a scenario and set them loose to discover the

biological/mathematical simulated solution in the cockpit.

Conclusions

drawn from Mr. Young's testimony differ, and the NTSB investigation are

incomplete. Yet this seems to suggest the increasing difficulty of

adequately simulating our complex machinery for correct operations under

real-world conditions.

✈ Re: Slide rules in the cockpit (White, [RISKS-22.32](#))

"Eric Remy" <eremy@rmwc.edu>

Wed, 30 Oct 2002 14:55:24 -0500

George White comments that "Years ago, pilots carried circular slide rules

to perform fuel and distance calculations."

Let me one of the many who comment that they still do, at least those of us

in general aviation. I was certainly trained to use an E6B when I got my

pilot's license about a year ago, and I've never used anything else. The

E6B can do time/speed/distance/fuel burn, crosswind corrections, temperature

and statute<->nautical mile conversions and a few others I forget at the

moment. It's more or less unchanged since WWII: cheap, durable, very fast

(I can often beat people using an "electronic E6B", and my instructor made me look slow.) and it has no batteries to die at the wrong moment. See

<http://www.sphere.bc.ca/test/sliderules/103-aristo-aviat-617.jpg>

for a photo of a typical one.

Eric D. Remy, Instructional Technology Coordinator
Randolph-Macon Woman's College (434) 947-8618 x7 eremy@rmwc.edu

✶ FDA permits use of ID chips in humans

Roger Clarke <Roger.Clarke@xamax.com.au>

Thu, 24 Oct 2002 08:44:21 +1000

This is a re-posting from the Politech list, with comments. The news report first, comments by Declan McCullagh second, comments by me third.

Date: Wed, 23 Oct 2002 10:10:45 -0400
From: Bob <bob@globaldevelopment.org>
To: declan@well.com
Subject: ID Chip's Controversial Approval

Wired.com, 23 Oct 2002

<http://www.wired.com/news/politics/0,1283,55952,00.html>

A surprise decision by the Food and Drug Administration permits the use of implantable ID chips in humans, despite an FDA investigator's recent public reservations about the devices.

The FDA sent chip manufacturer Applied Digital Solutions a letter stating that the agency would not regulate the VeriChip if it was used

for
"security, financial and personal identification or safety
applications,"
ADS said Tuesday.

But the FDA has not determined whether the controversial chip
can be used
for medical purposes, including linking to medical databases,
the company
added...

Declan McCullagh's Comments:

[There are two obvious questions: Should federal bureaucrats
forcibly
prevent a company from selling implantable chips of this sort?
And would it
be desirable for society to adopt these chips? I think the
answer to the
first is "no," and the answer to the second is also "no." I
would not stop
by government force or intervention people from using such
implants, but it
is reasonable to be concerned about what might happen with
widescale
adoption and speak out against it. Previous Politech message:
<http://www.politechbot.com/p-03135.html> --Declan]

Roger's Comments:

In the early 1990s, I wrote about what I call 'imposed
identifiers':
<http://www.anu.edu.au/people/Roger.Clarke/DV/HumanID.html#Imposed>
I also mused about prosthetisation of humans in:
<http://www.anu.edu.au/people/Roger.Clarke/SOS/Asimov.html>

For some years, I used the-chip-in-your-neck as a shock tactic
in a lot of
presentations. After the initial reaction of disbelief,
audiences were
forced to accept the line of argument that the institutionalised
would be
the first - prisoners, prisoners on day-release, senile dementia

patients.

Over a few short years, people have become inured to the shock-tactic. in response to press reports of the FDA announcement, there will be murmurs of 'oh, isn't it awful', and then parents will resume pumping chips into children (for what reason I've yet to work out), and Professor Warwick will become even more of a celebrity, with every failure reported in Wired Magazine, and hence the rest of the media, as another step forward.

I've not read the psychology literature about the Nazi assault on minorities; but the human race clearly has a genetic predisposition to rationalise the most dehumanising actions being taken in respect not only of other people, but even of one's self.

Any kind of external justification will do -- technological determinism, cost savings, prompt recognition of cadavers, instructions by the scientist conducting the experiment, or the desires of a belligerent government (Germany of the 30s and 40s, Argentina of the Generals, the Cambodia of Pol Pot, the U.S. of the here and now).

Roger Clarke <http://www.anu.edu.au/people/Roger.Clarke/> +61 2
6288 1472
Xamax Consultancy Pty Ltd, 78 Sidaway St, Chapman ACT 2611
AUSTRALIA
Visiting Professor, Uni of Hong Kong; Visiting Fellow,
Australian National U.

REVIEW: "Managing Information Security Risks", Alberts/

Dorofee

Rob Slade <rslade@sprint.ca>

Thu, 24 Oct 2002 08:00:40 -0800

BKMISROA.RVW 20020826

"Managing Information Security Risks", Christopher Alberts/
Audrey Dorofee,

2003, 0-321-11886-3, U\$54.99/C\$85.99

%A Christopher Alberts

%A Audrey Dorofee

%C P.O. Box 520, 26 Prince Andrew Place, Don Mills, Ontario
M3C 2T8

%D 2003

%G 0-321-11886-3

%I Addison-Wesley Publishing Co.

%O U\$54.99/C\$85.99 416-447-5101 fax: 416-443-0948

%P 471 p.

%T "Managing Information Security Risks: The OCTAVE Approach"

Part one is an introduction to risks and risk evaluation.

Chapter one is a

generic, and not particularly clearly written, outline of a
basic risk

analysis process. The OCTAVE (Operationally Critical Threat,
Asset, and

Vulnerability Evaluation) process is described in chapter two,
along with

various principles, factors (called attributes), and three
phases of outputs

(or deliverables) of the process.

Part two presents more details of the method. Chapter three
runs through

the outcomes and attributes again, but in a confusing fashion.

"Preparing

for OCTAVE," in chapter four, is a fairly generic outline of
preparation for

any kind of planning. Chapter five begins a list of the
individual

processes of OCTAVE, but essentially says that the company

should identify assets, threats and vulnerabilities. The creation of threat profiles, in chapter six, is the first part of the process that actually presents details and tools that might help in risk analysis. Chapter seven suggests that you identify key components of an asset, but, again, does not offer a specific process for doing so. Evaluating selected components, in chapter eight, seems to be merely subdividing asset threat analysis. Risk analysis is vaguely and briefly covered in chapter nine. Chapters ten and eleven contain pedestrian advice about developing a protection strategy.

Part three talks about variations to OCTAVE. Chapter twelve discusses the tailoring of OCTAVE, but since OCTAVE itself is rather vague, it is difficult to understand the options for alteration. Chapter thirteen asserts that OCTAVE is suitable for a variety of situations: since the process is so generic this is probably true. Chapter fourteen recommends reviewing or redoing an OCTAVE assessment from time to time-- just like any risk analysis.

Appendix B lists a variety of worksheets for risk analysis which could be quite useful.

This book is written in such a nebulous manner that it is difficult to day whether OCTAVE is an obscure method, or whether it is simply poorly explained.

copyright Robert M. Slade, 2002 BK MISROA.RVW 20020826
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

<http://victoria.tc.ca/techrev/~rslade>

or <http://sun.soci.niu.edu/>

REVIEW: "EW 101: A First Course in Electronic Warfare", David Adamy

Rob Slade <rslade@sprint.ca>

Wed, 30 Oct 2002 07:15:11 -0800

BKEW101.RVW 20020902

"EW 101: A First Course in Electronic Warfare", David Adamy, 2001,

1-58053-169-5, U\$89.00

%A David Adamy

%C 685 Canton St., Norwood, MA 02062

%D 2001

%G 1-58053-169-5

%I Artech House/Horizon

%O U\$89.00 800-225-9977 fax: 617-769-6334 artech@artech-house.com

%P 308 p.

%T "EW 101: A First Course in Electronic Warfare"

The book is based on the "EW 101" columns in the "Journal of Electronic Defense." It is, in fact, the first sixty such columns, structured into chapters and linked with additional material.

Electronic warfare (EW), as chapter one tells us, is intended to reserve the electromagnetic spectrum for friendly use, while denying

it to the enemy. We may be using the spectrum for communications,

such as radio, although the primary concern seems to be with remote

sensing, such as radar. EW is not concerned with such activities as

interception of enemy communications, or the design of directed energy weapons. Chapter two covers basic mathematics necessary for working with EW, such as logarithms (for working with decibel, or dB, representations) or spherical trigonometry. There is a very clear discussion of antenna characteristics, uses and design considerations in chapter three. Chapter four does the same thing for receivers, with an added examination of the concept of sensitivity. Processing of received signals is dealt with in chapter five, with a special concentration on display for and to the user (generally a pilot or signals officer). Chapter six looks at the multidimensional and multitechnology problem of the search for "threats" (as radio emitters are known in electronic warfare circles). "Low probability of intercept" (LPI) signals are the topic of chapter seven, which emphasizes the considerations in regard to spread spectrum technology. Various techniques for locating emitters are covered in chapter eight. Chapter nine deals with the many different types of jamming, and the power calculations necessary to concepts such as "burn through" range. Different types, missions, and purposes of decoys are discussed in chapter ten. Chapter eleven examines a wide variety of considerations involved in simulations.

As the title notes, for those interested in an introduction to the topic, this book is an informative and interesting tutorial, readable, and with a minimum of mathematics necessary to the topic.

copyright Robert M. Slade, 2002 BKEW101.RVW 20020902
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca

pl@canada.com

[http://victoria.tc.ca/techrev
~rslade](http://victoria.tc.ca/techrev/~rslade)

or

<http://sun.soci.niu.edu/>

★ **REVIEW: "Disaster and Recovery Planning", Joseph F. Gustin**

Rob Slade <rslade@sprint.ca>

Fri, 25 Oct 2002 07:46:27 -0800

BKDRPGFM.RVW 20020825

"Disaster and Recovery Planning", Joseph F. Gustin, 2002,
0-13-009289-4

%A Joseph F. Gustin

%C One Lake St., Upper Saddle River, NJ 07458

%D 2002

%G 0-13-009289-4

%I Prentice Hall

%O U\$ +1-201-236-7139 fax: +1-201-236-7131

%P 304 p.

%T "Disaster and Recovery Planning: A guide for Facility
Managers"

Despite the title, and a number of the topics covered, this book
seems

to have more to do with business continuity than disaster
planning.

Chapter one does talk about disaster types (and lists not-so-
recent

disasters), and has a rough outline of basic parts of the
planning

process. Some US regulations that may influence plans are
discussed

in chapter two. Immediate emergency response is reviewed in
chapter

three. Chapter four talks about types of disasters again (and,
again,

the examples are fairly old). Fire protection and response, in

chapter five, is very uneven in the level of detail, and concentrates heavily on technicalities in regard to exits. Bomb threat response, in chapter six, emphasizes searching techniques. Evacuations are covered in chapter seven. Chapter eight encompasses earthquakes, with the major emphasis being on structural design to prevent damage. Computer and data protection, in chapter nine, is poor and brief. Chapter ten is a simplistic look at power requirements. There is a set of generic loss prevention strategies in chapter eleven. Crisis planning, in chapter twelve, is primarily concerned with handling the media. Chapter thirteen, putting the plan together, is pedestrian, but reasonably comprehensive.

The final chapter, on managing the recovery, is very thorough.

For those new to business continuity planning, this book does provide some basic outlines and tips. But for those who have worked with disaster or continuity planning to any extent, there is nothing new here.

copyright Robert M. Slade, 2002 BKDRPGFM.RVW 20020825
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

<http://victoria.tc.ca/techrev/~rslade> or <http://sun.soci.niu.edu/~rslade>

✶ CFP, Security and Control of IT in Society: SCITS III

Rob Slade <rslade@sprint.ca>
Thu, 24 Oct 2002 10:37:23 -0800

Security and Control of IT in Society (SCITS) III
Special Track on SEC'2003
18th IFIP International Information Security Conference
Athens Chamber of Commerce and Industry
26-28 May 2003, Athens, Greece
www.sec2003.org

[Contact scits3@cs.kau.se for instructions. Papers must be received by November 12, 2002. PGN]

Papers offering novel research contributions in any aspect of IT Misuse and the Law are solicited for submission to this Special Track of the 18th IFIP International Information Security Conference. Papers may present theory, applications or practical experiences (e.g. case studies) on topics including, but not limited to:

- High-tech crime prevention, detection, and investigation
- International Cooperation in fighting high-tech crime
- Computer Forensics
- IT law for preventing Misuse
- Social and Legal Risks through interception and tracking technologies -
 - Data retention vs. privacy in communication and archived systems - Crypto
 - / Anonymity debate - Protecting users/uses by Privacy-Enhancing Technologies
- Perception of security in society
- Behavioral issues of information security
- Security awareness
- Users' security responsibilities
- Critical Information Infrastructure Protection and Social Implications -
 - Adequacy and Inadequacy of the Law - Multilateral Security - Social, legal and ethical aspects of IT security



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

[ACM](#) Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 34

Monday 4 November 2002

Contents

- [Prior Florida voting woes spawn pre-election frenzy](#)
[Charles P Schultz](#)
- [Election counting conclusions](#)
[Paul D. Smith](#)
- [Risks of dual-boot systems](#)
[Paul Schreiber](#)
- [Windows daylight saving and file time-stamp](#)
[Chris Jakeman](#)
- [Microsoft court ruling leaked early through security blunder](#)
[Keith Rhodes](#)
- [Exam software -- does it get a passing grade?](#)
[David Leshner](#)
- [\\$3,200 tuition listed on bill as 'Taco Bell'](#)
[Fuzzy Gorilla](#)
- [Turnpike commuters play "Where's the Fast Lane?"](#)
[Monty Solomon](#)
- [BBC News: Fake bank website cons victims](#)
[Chris Leeson](#)
- [GAO: Government Agencies Adhering To Privacy Laws](#)
[Monty Solomon](#)

- [REVIEW: "Ethical Issues of Information Systems", Ali Salehnia](#)
[Rob Slade](#)
 - [REVIEW: "Computer Security Handbook", Seymour Bosworth/M. E. Kabay](#)
[Rob Slade](#)
 - [CARDIS '02: 5th Smart Card Research/Advanced Application Conference](#)
[Alex Walker](#)
 - [Formal Methods Europe 2003 cfp](#)
[Diego Latella](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✂ Prior Florida voting woes spawn pre-election frenzy

Schultz CharlesP-ECS013 <ecs013@motorola.com>

Mon, 4 Nov 2002 17:45:26 -0500

Due to the problems we have had in recent history both with manual voting, and the more recent electronic voting systems put into place, it became possible to "pre-vote" here in South Florida - most notably in Miami-Dade and Broward counties. Over the past few days the reported waiting times for "early voters" has steadily risen to today's peak of 2-3 hours. In spite of thousands of people waiting in lines and casting their votes, we apparently have not yet begun the "election."

<http://www.miami.com/mld/miami/4442229.htm>

As it turns out, there seem to be no lessons learned, as the same issues that caused problems with electronic voting in the primaries (lack of training, poor facilities, lack of equipment to name a few) are still in force during this early election period. I am wondering if SO many people

have already voted now that there will be short lines on election day, or if the problems are going to be magnified by the even larger number of people who still have not voted. The voting manufacture seems to already be covering its tracks by explaining why voters should expect delays and voting times of up to 25 minutes per person. http://www.essvote.com/index.php?section=news_item&news_id=84

I certainly have some concerns regarding the integrity of the voting process and the votes themselves, especially those that are cast during this early voting period. During our primaries, we had episodes of votes tallied for a precinct being greater than the registered voters in that precinct, lower than expected votes (sometimes 0) were recorded for precincts with traditionally good voter turnout and poor accounting of individual voting machines [The Herald Saturday, September 14, 2002]. So now that this process is spread over a period of days, some new risks have been introduced :

- retention of information by voting machines (e.g. does machine get accidentally reset from one day to the next)
- influence of "early voting" polls have on the voting taking place on the "official" election day
- duplicate voting (e.g. person votes on multiple days by registering with different workers)
- memory capacity of individual machines (e.g. can votes get overwritten if

volume is too high for an individual machine?)

- the integrity of the counting votes from individual machines
(I don't know whether this is taking place on a daily basis, or must be delayed

until the end of election day)

- and maybe an even higher than usual number of recounts and finger

pointing which can be based on this unusual early voting practice, which

will then expose further problems when results are overturned, etc.

Charles P. Schultz, North Miami Beach, FL

✶ Election counting conclusions

"Paul D. Smith" <PDS@dataconnection.com>

Thu, 10 Oct 2002 09:07:09 +0100

Many contributors have pointed out the extremes of election counting requirements, from the British "1 or 2 contests per ballot, count by hand" from the US "Many contests per ballot, count electronically". This is a thread that could run and run but we can draw the various conclusions together and define the simple requirements for a good voting system.

1. A hand count, with observers from the contesting parties present, is the safest and fairest way to count ballots, especially close, or suspect ballots.

2. Where a simple, accurate, electronic system can be used, then it may be but is **MUST** be possible to back this up with a hand count, using the original ballot papers, in the event of any irregularities or concerns from the candidates or voters.

3. The method of indicating a choice on a ballot should be simple and the results immediately visible to, and correctable by, the voter. The voter indicating "OK", whether by depositing the ballot in a box or pressing a lever or whatever, should have **NO** affect on the voting slip - for example this is **NOT** the time to punch out the holes indicating the selections because the act of punching could fail leaving the voter with no indication of their spoiled or incorrect vote.

Note that I have deliberately not commented on the risks of voting for many contest (did somebody mention 45!) in one ballot. This is a matter for the residents of the ballot area to consider -- do they want to vote at this degree of choice or are they happy to delegate to a representative?

[The answers may well be No! and No! in many cases. PGN]

I believe that pretty much covers the ideal voting system. All flaws in existing systems result because the system fails to address one or more of the three criteria above.

⚡ Risks of dual-boot systems

Paul Schreiber <shrub@mac.com>

Sat, 2 Nov 2002 15:14:29 -0800

A friend of mine has a dual-boot PC running Windows 98 and Windows 2000. Last week, it was booted into Windows 98 when the daylight savings time changeover occurred.

Windows 98 was smart enough to automatically adjust the clock back an hour. However, when he rebooted into Windows 2000, it adjusted the clock back a second hour.

This could lead to many problems if not caught, including alarms going off at the wrong time, scheduled tasks running at inconvenient hours, incorrect email headers and much more destructive behaviour if used in a mission-critical situation.

⚡ Windows daylight saving and file time-stamp

"Chris Jakeman (Bigfoot)" <cjakeman@bigfoot.com>

Sun, 3 Nov 2002 21:48:22 -0000

Discovered today that a misbehaving program was due to a strange behaviour in Windows. (Can't find any reference to this on comp.risks.)

When the computer clock changes due to Daylight Saving Time (we gained an hour a week ago in the UK), Windows also changes the time stamp of all its files by an hour.

This came to light when synchronising files between a Unix webserver and a Windows copy of the website, using Dreamweaver.

Microsoft discusses this behaviour in its Knowledge Base at <http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q129574>&

but apparently sees nothing wrong in providing a time stamp that changes.

One query: When Samba is used to make Unix files look like Windows ones, does it fiddle the time stamp to emulate this bizarre behaviour?

Risks: On networks that mix Unix and Windows, this problem might screw up any utility that relies on timestamps such as incremental backups and source code control systems.

Microsoft court ruling leaked early through security blunder

Keith Rhodes <rhodesk@gao.gov>

Mon, 4 Nov 2002 09:24:17 -0800 (PST)

Court staffers didn't realize that the ruling placed on their servers became public knowledge two hours early -- even though it wasn't posted on their Web site. [Source: Patick Gray, *ZDNet Australia*, 4 Nov 2002; PGN-ed]

<http://zdnet.com.com/2100-1104-964415.html>

[Interesting competition of ideas: They want to put the file on the Web so that people will find it, but they think it will be safe until they release it if they put it on the Web because no one will be

able to find
it. Keith]

[The judgment went up at 2:40pm EST Friday, prior to its
intended
release time of 4:30pm EST. The URL was fairly obvious, and
the
directory was freely browsable. PGN]

✶ Exam software -- does it get a passing grade?

David Lesher <wb8foz@nrk.com>
Wed, 30 Oct 2002 21:04:43 -0500 (EST)

Georgetown Law Center lets students use their laptops on exams,
IFF they
have installed a package called "SofTest" from ExamSoft. It
blocks other
uses of the laptop, but allows the exam to be taken on it. Or so
it sez..

Known problems include:

- * Only works on WinDoze systems; forget that Ti OSX PB, or any Linux laptop.
- * Requires the laptop have a floppy drive
- * Sometimes fails during exams.

But with so many unemployed nerds headed back to grad schools,
it's easy to
imagine OTHER problems. What about VMware? What about a
determined
programmer who decides hacking code is easier than grok-ing
Feist vs. Rural
Telephone? Suppose she writes a Examsoft-specific virus that
stay dormant
until the middle of the exam....then bombs all the OTHER
machines in the
class.

And most of all, who watches the watcher?

Is this an indirect way to get more attorneys who can code?

✦ \$3,200 tuition listed on bill as 'Taco Bell'

"Fuzzy Gorilla" <fuzzygorilla@euroseek.com>

Thu, 10 Oct 2002 15:24:43 -0400

A glitch in vendor software erroneously caused some University of Wisconsin-La Crosse room/board/tuition payments to be listed as charges from

Taco Bell on credit-card statements. [Source: AP item, 10 Oct 2002; PGN-ed]

http://dailynews.yahoo.com/news?tmpl=story2&u=/ap/20021010/ap_on_fe_st/_3

✦ Turnpike commuters play "Where's the Fast Lane?"

Monty Solomon <monty@roscom.com>

Mon, 4 Nov 2002 15:04:00 -0500

The Fast Lanes (like EZPass lanes) are not always in the same configuration

in Massachusetts, sometimes on one side, sometimes in the middle, sometimes

combined with exact-change lanes, sometimes right between two exact-change

lanes. This seems to be resulting in long lines where they could be avoided

by a more sensible layouts. "This results in vehicles switching lanes via

the Fast Lane/exact change lane like crazed motorized salmon

running

upstream." [Source: Mac Daniel, *The Boston Globe*, 3 Nov 2002;
PGN-ed]

[http://www.boston.com/dailyglobe2/307/metro/
Pike_commuters_play_Where_s_the_Fast_Lane_.shtml](http://www.boston.com/dailyglobe2/307/metro/Pike_commuters_play_Where_s_the_Fast_Lane_.shtml)

✶ BBC News: Fake bank website cons victims

"LEESON, Chris" <CHRIS.LEESON@london.sema.slb.com>

Tue, 8 Oct 2002 15:44:10 +0100

[It seems that the old Nigerian scam is becoming more hi-tech
(although Web
site spoofing and e-mail scams are hardly news in RISKS). CL]

As revealed by BBC Radio5Live, West African spam scammers used
an unclaimed
Web domain of a British bank's online service that looked
genuine. and found
still more gullible people. The UK National Criminal
Intelligence Service
notes that at least two Canadians had lost more than \$100,000
after being
gulled by the fake Web site. In response to letters, e-mail,
and now Web
sites (one has been shut down), this type of scam somehow
continues to be
profitable for the scammers. [Greed? Stupidity? ...]

"One of the first companies to fall victim to website spoofing
was net
payment service Paypal. Con-men set up a fake site and asked
people to
visit and re-enter their account and credit-card details because
Paypal had
lost the information. The Web site link included in the e-mail
looked
legitimate but in fact directed people to a fake domain that

gathered

details for the con-men's personal use." [Source: BBC News Website; PGN-ed]

<http://news.bbc.co.uk/1/hi/technology/2308887.stm>

GAO: Government Agencies Adhering To Privacy Laws

Monty Solomon <monty@roscom.com>

Thu, 31 Oct 2002 18:12:50 -0500

On 30 Oct 2002, the General Accounting Office issued a report "Information Management: Selected Agencies' Handling Of Personal Information" finding that the Departments of Agriculture, Education, Labor, and State generally adhere to government privacy laws. "The report found that agencies' handling of information varies and that a wide range of government personnel have access to the information, but by and large, the agencies follow current privacy laws." (Information considered included names, phone numbers, addresses, SSNs, financial and legal data, and demographic information, provided for a specific purpose such as to receive benefits, obtain services or loans, or participate in a specific federal program.)

[Source: Eric Chabrow, *InformationWeek*, 30 Oct 2002; PGN-ed]

<http://news.lycos.com/news/story.asp?section=Politics&storyId=556059>

[RISKS always seeks positive items that do not represent horrible cases

involving security, privacy, reliability, safety, survivability, financial

losses, etc. It is always startling how few really constructive cases

there are. On the other hand, the GAO report clearly does not imply that

there are no potential problems in those four departments.
PGN]

✶ REVIEW: "Ethical Issues of Information Systems", Ali Salehnia

Rob Slade <rslade@sprint.ca>

Tue, 29 Oct 2002 08:01:28 -0800

BKETHISS.RVW 20020831

"Ethical Issues of Information Systems", Ali Salehnia, 2002,
1-931777-15-2

%E Ali Salehnia

%C 1331 E. Chocolate Ave., Hershey, PA 17033-1117

%D 2002

%G 1-931777-15-2

%I IRM Press/Idea Group

%O U\$ 800-345-432 717-533-8845 fax: 717-533-8661 cust@idea-
group.com

%P 301 p.

%T "Ethical Issues of Information Systems"

As with any collection of essays, there isn't much of a common thread between the pieces. However, in this case, there isn't even an attempt to set up a structure, or group the papers into subjects.

In chapter one, Internet privacy is very poorly defined, and then we are told that an opinion poll and an unqualified panel have decided that there are five primary privacy concerns. Chapter two points out that some companies might not benefit from establishing their own global information

network. There are some brief thoughts on uniform contract codes and jurisdiction in chapter three. A poorly documented study, in chapter four, indicates that neural nets do better than random chance at predicting moral attitudes from sets of disjoint questions. A study in chapter five finds that when you ask people ethical questions, and then ask why they decided the way they did, morals are a strong factor. Chapter six is much more detailed than most of the other papers, and uses stories of the automation of stock markets in China, Russia, and Chile to point out benefits and problems with electronic auction systems. Poor people, and countries, have less technology with which to advance themselves, we are told in chapter seven. Chapter eight points out that we should do a proper risk management analysis if we are relying on e-commerce. After careful study and analysis, chapter nine finds (from self-reports) that people who have more opportunities to pirate software are more inclined to think that the practice is OK. Chapter ten tells us that there are problems with the quality of software. There is a brief, but not bad, introduction to information warfare in chapter eleven. Chapter twelve is a fictional "conversation" on the ethics of teachers and researchers. People who copy or pirate software tend to think that it is OK to hurt a big guy (a corporation) because hurting a big guy helps the little guy (individual), we are told in chapter thirteen. Chapter fourteen asserts the need for public policy in relation to e-commerce. Soren Kierkegaard theorized that remote

information keeps people from forming local relationships, and chapter fifteen relates this to the Internet. There are some interesting stories in chapter sixteen about competitive intelligence or industrial espionage. The examination of the ethics of outsourcing, in chapter seventeen, is actually more about fraud. Chapter eighteen looks at the Nietzschean concept of authenticity; that moral choices need to come from within the individual; but does not examine the problems that have been analyzed in regard to the very similar concepts involved in Kohlberg's level six of ethical development. A variety of views of ethics are listed in chapter nineteen. A compilation of the arguments for and against the Australian Internet censorship bill is given in chapter twenty. Chapter twenty tells us that a couple of researchers asked for an opinion survey on whether or not using genetic tests for finding genetic diseases was ethical.

Aside from the lack of structure and depth, this book has a number of problems. Some are technical: the proofreading is a definite problem, with famous names being spelled incorrectly and punctuation appearing in bizarre places. As demonstrated by the bibliographies attached to each paper, the authors are attempting to deal with issues involving technology without having read standard technical references. (An additional bothersome point is that all of these papers seem to have been collected from a very limited pool of resources: all have appeared in Idea Group books or periodicals.)

While the individual papers may raise some issues that might be

interesting
for discussion, ultimately the book does not contribute to the
computer
ethics debate. Pretty much everything in the book is either
glaringly
obvious, or has been discussed to death in other works.

copyright Robert M. Slade, 2002 BKETHISS.RVW 20020831
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

<http://victoria.tc.ca/techrev> or <http://sun.soci.niu.edu/~rslade>

REVIEW: "Computer Security Handbook", Seymour Bosworth/ M. E. Kabay

Rob Slade <rslade@sprint.ca>
Mon, 4 Nov 2002 08:03:31 -0800

BKCMSCHB.RVW 20020911

"Computer Security Handbook", 2002, Seymour Bosworth/M. E. Kabay,
0-471-41258-9

%E Seymour Bosworth sybosworth@aol.com

%E M. E. Kabay mkabay@norwich.edu

%C 5353 Dundas Street West, 4th Floor, Etobicoke, ON M9B 6H8

%D 2002

%G 0-471-41258-9

%I John Wiley & Sons, Inc.

%O U\$75.00 416-236-4433 fax: 416-236-4448

%P 1224 p.

%T "Computer Security Handbook, Fourth Edition"

There are many recognizable (and a lot more not so recognizable)
names
in the list of contributors. Authors such as Rebecca Bace, Donn
Parker, and William Stallings stand out as people who have
something

worth saying, and can say it well. Other names are associated with less worthy works.

Chapter one states that the purpose of the handbook is to describe information system security risks, the measures for mitigating those risks, and the techniques for managing security risks. In a sense, it does that, but risk management is not the whole of computer security. Even if the title of the book were to confine itself to risk management, one would still have to say that, overall, there are other works that cover the field more completely, with less wasted verbiage.

There has been an attempt to remove the limiting of previous editions to topics relevant to "big iron." However, new technologies still seem to get short shrift.

Part one looks at foundations of computer security, with papers examining the history and mission of security (actually just history of computers), law and computer forensics (random collection of legal issues, almost nothing on forensics), common language for computer incident information (proposal with no proof that it will either cover all incidents or assist with dealing with incidents), surveys of computer crime (lots of material on how studies should be conducted, and uncritical reports of some studies), and new framework for security (Donn Parker says we are missing pieces of security).

Threats and vulnerabilities are reviewed in part two, including essays on the psychology of computer criminals (mostly good but some questionable observations and theories about black hats),

information warfare (information systems can be attacked--surprise!), penetrating systems and networks (there are different ways to get unauthorized access), malicious code (traditional models and some recent examples of viruses), mobile code (some aspects of ActiveX and scripting), denial of service attacks (reasonable overview of various types--and some unrelated exploits), intellectual property (random legislation and thoughts), e-commerce vulnerabilities (various weaknesses), and physical threats (generic disaster recovery).

Part three covers preventive technical defenses, containing topics such as protecting information infrastructure (generic security, mostly physical), identification and authentication (brief introduction), operating system security (good introduction to access control), local area networks (random thoughts), e-commerce safeguards (legal protections and vague ideas), firewalls (confused grab bag), protecting Internet systems (basic concepts), protecting web sites (broad but not deep), public key infrastructure (basic components, but no more), antivirus technology (simplistic look at scanning), software development (simplistic look at the software development life cycle), and piracy (piracy is going on and we have to find some way to stop it).

Human factors, in part four, looks at standards for security products (verbose description of the Common Criteria components), security policy guidelines (miscellaneous related documents), security awareness (do interesting seminars), ethics (vague), employment

policies (grab bag), operations security (and another), Internet use policies (yet again), working with law enforcement (generic and poorly structured), social psychology (redoing the security awareness article with extra psychological jargon), and auditing computer security (a checklist).

Part five's look at detection is brief, with intrusion detection (excellent introduction), monitoring (you should log stuff), and application controls (database integrity).

Remediation reviews computer emergency response teams (generic), backups (pedestrian), business continuity planning (have a plan), disaster recovery (repeat previous), and insurance (get some) in part six.

Part seven examines management's role, including management responsibilities (you could be liable), developing policies (generic), risk assessment (assess risks), and Y2K (management is now onside-- yeah, right).

Other considerations, such as medical records (good introduction and discussion of the issues), using encryption internationally (laws differ), censorship (random thoughts), privacy (various laws), anonymity (psychological ponderings), and the future (various thoughts) make up part eight.

There is useful material in the work, but it is difficult to abstract the good from the mundane unless you are already quite expert in the field. The newcomer would be advised to get some basic training or reading before attempting to deal with this work, but the expert will be able to find some useful nuggets.

copyright Robert M. Slade, 2001, 2002 BKCMSCHB.RVW 20020911
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com
<http://victoria.tc.ca/techrev/~rslade> or <http://sun.soci.niu.edu/~rslade>

★ **CARDIS '02: 5th Smart Card Research/Advanced Application Conference**

Alex Walker <alex@usenix.org>
Mon, 04 Nov 2002 09:55:37 -0800

5th Smart Card Research and Advanced Application Conference
San Jose, CA, 21-22 Nov 2002
<http://www.usenix.org/events/cardis02/>

Keynote speaker Vincent Cordonnier, LIFL; 14 refereed papers; panel discussions; Work-In-Progress reports as well as ample opportunities to informally interact with fellow attendees and speakers. Unlike events devoted to commercial and application aspects of smart cards, the CARDIS conferences bring together researchers who are active in all aspects of the design, validation, and application of smart cards. The breadth of smart card research stimulates a synergy among disparate research communities, making CARDIS an ideal opportunity to explore and learn from the latest research advances.

Peter Honeyman, CITI, University of Michigan
CARDIS '02 Program Chair

Alex Walker, Production Editor, USENIX Association
2560 Ninth Street, Suite 215, Berkeley, CA 94710 1-510/528-8649
x33

✶ Formal Methods Europe 2003 cfp

Diego Latella <diego.latella@cnuce.cnr.it>
Mon, 04 Nov 2002 11:37:44 +0100

FM 2003: the 12th International FME Symposium
Pisa, Italy -September 8-14, 2003
Papers must be submitted electronically by 7 Mar 2003.
<http://fme03.isti.cnr.it/fme-cfp.htm>

FM 2003 is the twelfth in a series of symposia organized by Formal Methods Europe, an independent association whose aim is to stimulate the use of, and research on, formal methods for software development. These symposia have been notably successful in bringing together a community of users, researchers, and developers of precise mathematical methods for software development as well as industrial users.

Formal methods have been controversial throughout their history, and the realisation of their full potential remains, in the eyes of many practitioners, merely a promise. Have they been successful in industry? If so, under which conditions? Has any progress been made in dispelling the scepticism that surrounds them? Are they worth the effort? Which aspects of formal methods have become so well established in industrial practice that they have lost the "formal method" label in the meanwhile?

FM 2003 aims to answer these questions, by seeking contributions not only from the Formal Method community but also from outsiders and even from skeptical people who are most welcome to explain, document, and motivate the source of their reluctance. We are confident that a wide spectrum of experiences and a loyal contrasting of opinions will foster a better and deeper understanding, if not a wider adoption of Formal Methods.

Far from restricting the focus of the conference, however, FM 2003 also welcomes papers with strong theoretical content that establish a connection with the practice of formal methods. [PGN-ed]

Dott. Diego Latella, Consiglio Nazionale delle Ricerche
Area della Ricerca di Pisa - Ist. di Scienze e Tecnologia
dell'Informazione - ISTI

Via G. Moruzzi, 1 - I56124 Pisa, ITALY

phone: +39 0503152982 or +39 348 8283101

fax: +39 0503138091 or +39 0503138092

email: Diego.Latella@cnuce.cnr.it

<http://www.cnuce.pi.cnr.it/people/D.Latella>



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

[ACM](#) Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 35

Tuesday 5 November 2002

Contents

- [Online job listing an ID theft scam](#)
[Monty Solomon](#)
- [Want a driver's license? How about an ID card instead?](#)
[Mark Richards](#)
- [The FBI Has Bugged Our Public Libraries](#)
[Bill Olds via Forno and Farber](#)
- [What if they held an election and the pundits had nothing to say?](#)
[NewsScan](#)
- [Vote-by-mail in Oregon](#)
[Andrew Morton](#)
- [Software leaves encryption keys, passwords lying around in memory](#)
[Peter Gutmann via Monty Solomon](#)
- [Risks of non-obvious user interfaces](#)
[Harry Erwin](#)
- [Why Telemarketing Is Evil](#)
[Neil McManus via Monty Solomon](#)
- [Re: BBC News: Fake bank website cons victims](#)
[Hal Murray](#)
- [Re: Windows daylight saving and file time-stamp](#)
[Graham Mainwaring](#)

- [Re: Risks of dual-boot systems](#)
 - [Scott Nicol](#)
 - [Tony Finch](#)
 - [Colin Andrew Percival](#)
 - [Nick Rothwell](#)
 - [David Crooke](#)
 - [Wireless networking and security: CERIAS/Accenture roundtable](#)
 - [Gene Spafford](#)
 - [REVIEW: "Internet Security Dictionary", Vir V. Phoha](#)
 - [Rob Slade](#)
 - [Digital System Design DSD 2003 cfp](#)
 - [Henry Selvaraj](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Online job listing an ID theft scam

Monty Solomon <monty@roscom.com>

Tue, 5 Nov 2002 01:29:52 -0500

'Background check' used to steal full slate of personal info
By Bob Sullivan, MSNBC, 4 Nov 2002

It was just the job lead Jim needed: a marketing manager position with Arthur Gallagher, a leading international insurance broker. And only days after Jim responded to the job posting on Monster.com, a human resources director sent along a promising e-mail. We're interested in you, the note said. The salary is negotiable, the clients big. In fact, the clients are so valuable and sensitive that you'll have to submit to a background check as part of the interview process. Eager for work, Jim complied -- and sent off just about every key to his digital identity, including his age,

height,
weight, Social Security number, bank account numbers, even his
mother's
maiden name. IT WAS ALL JUST an elaborate identity theft scam
designed to
prey on the most vulnerable potential victims - the increasing
ranks of the
unemployed. ...

<http://www.msnbc.com/news/830411.asp>

✶ Want a driver's license? How about an ID card instead?

Mark Richards <mark.richards@massmicro.com>

Mon, 4 Nov 2002 21:59:35 -0500

As reported by the Associated Press, 4 Nov 2002, the
Massachusetts Registry
of Motor Vehicles' new online renewal system issued Massachusetts
identification cards instead of renewed driver's licenses to
3,600 drivers
requesting renewals between 21 and 23 Oct. The RMV's request to
Digimark
Corporation (which prints the licenses) apparently erroneously
included a
field indicating ID cards had been requested. The problem was
then caught
and corrected. (Each license costs the RMV \$1.77.) [PGN-ed]

[Not mentioned in the article:] The recent (but now former) head
of the RMV,
Daniel Grabauskas, is a political appointee who claims to have
reformed the
agency and improved efficiency. On that basis, he is running
for State
Treasurer. On the eve of a State-wide election, this revelation
of goof
does not have the most beneficent timing.

[http://www.boston.com/dailynews/308/region/
Online_license_renewals_fouled:.shtml](http://www.boston.com/dailynews/308/region/Online_license_renewals_fouled:.shtml)

⚡ The FBI Has Bugged Our Public Libraries (from Dave Farber's IP)

Richard Forno <rforno@infowarrior.org>
Tue, 05 Nov 2002 16:40:41 -0500

[Source: A long and provocative article by Bill Olds, *The Hartford Courant*, 3 Nov 2002, excerpted here; PGN]
<http://www.ctnow.com/features/lifestyle/hc-privacy1103.artnov03col.story>

Some reports say the FBI is snooping in the libraries. Is that really happening? Yes. I have uncovered information that persuades me that the Federal Bureau of Investigation has bugged the computers at the Hartford Public Library. And it's probable that other libraries around the state have also been bugged. It's an effort by the FBI to obtain leads that it believes may lead them to terrorists.

Many members of the public regularly use computers in libraries to access the Internet for research purposes or to locate information about particular interests. It's also not uncommon for students and others to communicate with friends and relatives through e-mail from there.

The FBI system apparently involves the installation of special software on the computers that lets the FBI copy a person's use of the

Internet and their e-mail messages. (Don't ask me how I know about this because I can't reveal how I was able to collect the information.) Members of the public who use the library have not been informed that the government is watching their activities. It's not just the computers. Circulation lists that show which books someone borrowed are also accessible to the government.

What are the Hartford librarians saying?

"I can't disclose that we were presented with anything," said Louise Blalock, Hartford's head librarian.

I asked Mary W. Billings, the library's technical services manager, if the FBI had given her a subpoena or a court order for library information. Her response: "I cannot answer that question." [...]

[Bill Olds, c/o *The Hartford Courant*, Features Department, 285 Broad St., Hartford, CT 06115 or docbillo@yahoo.com]

⚡ What if they held an election and the pundits had nothing to say?

"NewsScan" <newsscan@newsscan.com>
Tue, 05 Nov 2002 08:14:58 -0700

Modern elections have become so much more than counting the votes: they've become opportunities for political analysts to show off by projecting the results before the votes are counted, as well as by using demographic data

and exit polls to explain to the politically unwashed what it all really means, deep down. But there's one little glitch this time: last-day computer problems with the new system of the Voter News Service, the consortium of news organizations that does the exit polling. CNN's Tom Hannon said of the new system yesterday: "It is brand-new and has never been test-driven. This is the equivalent of a NASA space shot without any test runs. We are going to learn a few things tomorrow night in real time." [Great.] Gerald M. Boyd of the New York Times says: "The use of exit polls has been particularly important in terms of trying to get a sense of national trends or moods, so without it, we would have to do the best we can." [And the rest of us will just have to soldier on bravely.] [*The New York Times*, 5 Nov 2002;

NewsScan Daily, 5 November 2002]

<http://partners.nytimes.com/2002/11/05/politics/campaigns/05VNS.html>

[A tangible benefit of exit polls arises in the use of today's all-electronic voting systems that have essentially zero accountability

that your vote is correctly recorded and counted: if the exit polls differ

radically from the officially tabulated reported results, then one might

have good reason to suspect fraud that would otherwise be largely

undetected, or perhaps some egregious internal mishaps. PGN]

[The *Times* item was also noted by Ian Alderman, who included this quote:

"Without all the states, the papers count on the demographic and other

details from the national poll to explain the reasons for the election

results in their articles the next day. But Mr. Savaglio said Voter News

Service could analyze the data for its national poll only after it

finished analyzing its data by state. That makes the national poll the

most vulnerable to any problems."

PGN]

✶ Vote-by-mail in Oregon (Re: Smith, [RISKS-22.34](#))

andrew morton <drewish@katherinehouse.com>

Tue, 05 Nov 2002 12:12:40 -0800

The ballot originally mentioned was the state of Oregon's. In Oregon, every ballot is essentially an absentee ballot, they're mailed out several weeks before the Nov 5th deadline, voters complete the optically scanned ballots at their leisure and in the privacy of their own home. Voters are allowed plenty of time to make their decisions and ensure that the ballot is marked correctly. The voted ballot can either be dropped off at a collection point or mailed so that (regardless of postmark) it is received by 8:00 pm on election day. More details about the system can be found on the Secretary of State's website.

<http://www.sos.state.or.us/executive/policy-initiatives/vbm/execvbm.htm>

✶ Software leaves encryption keys, passwords lying around in

memory

Monty Solomon <monty@roscom.com>

Wed, 30 Oct 2002 22:31:46 -0500

<http://online.securityfocus.com/archive/82/297827>

Date: Thu, 31 Oct 2002 05:11:31 +1300 (NZDT)

From: pgut001@cs.auckland.ac.nz (Peter Gutmann)

Subject: Software leaves encryption keys, passwords lying around in memory

The following problem was first pointed out (in private mail) by Michael

Howard from Microsoft. His writeup is now available at

<http://msdn.microsoft.com/library/en-us/dncode/html/secure10102002.asp>.

From a representative check of a few widely-used open source crypto programs, this affects quite a bit of software.

The problem he points out is that clearing sensitive information such as

encryption keys from memory may not work as expected because an optimising

compiler removes the `memset()` if it decides it's redundant.

Consider for

example the following:

```
int encrypt( const void *key )
{
    puts( key );      /* Normally we'd encrypt here */
}
```

```
void main( void ) /* Because we can */
```

```
{
    char key[ 16 ];
```

```
    strcpy( key, "secretkey" );
```

```
    encrypt( key );
```

```
    memset( key, 0, 16 );
```

}

When compiled with any level of optimisation using gcc, the key clearing call goes away because of dead code elimination (see the MSDN article for more details on this, which uses VC++ to get the same effect). While you can kludge enough stuff around a custom memory-clear call to fool the optimiser (hacks with 'volatile', touching the memory after it's cleared and hoping the optimiser is fooled, etc etc) there's no guarantee that it'll work for anything but the compiler(s) you happen to test it with - any future enhancement to the optimiser may turn it back into a nop. What it really needs is the addition of a #pragma dont_remove_this_code_you_bastard in the compiler. Until then, a lot of security code will be affected by this problem.

[In RISKS, I tend never to alter British spellings. However, in American English, an "optimiser" must be the ultimate miser.]

✶ Risks of non-obvious user interfaces

Harry Erwin <herwin@theworld.com>
Tue, 5 Nov 2002 16:02:05 +0000

I'm using a product called WebCT to web-enable a couple of classes that I'm teaching in the UK. I find I have students listed by WebCT as not having submitted a project, but when I download the project files, why there they

are! Apparently the students have to take some positive action other than simply submitting the project for the software to believe they submitted it. There doesn't appear to be any mechanism, either, for logging marks for students who did this or submitted the project via some other mechanism. I used to teach at George Mason University (VA), where we used a similar package developed at the University of Maryland. The difference was that the UMD developers actually seemed to have thought through this stuff.

✶ Are you bothered by telemarketing?

Monty Solomon <monty@roscom.com>

Wed, 30 Oct 2002 01:23:49 -0500

Why Telemarketing Is Evil

Neil McManus, CHEAT SHEET, wired.com, Issue 10.11 - Nov 2002

Telemarketers may be relentless, exasperating, even unethical. But you have to give them this: They're good. With the help of technology - everything from autodialing software to cheap overseas labor connected by fiber optics - they've turned phone solicitation into a \$270 billion industry. The key to the telephonic onslaught is predictive dialing, a breakthrough of the mid-'90s. These systems churn through huge databases of phone numbers, weeding out busy signals and out-of-service numbers, and routing answered calls to agents. They are mercilessly efficient: Out of an 8-

hour day,
agents can work the phones a staggering 7.2 hours. One loan
company calling
deadbeat borrowers boosted "promises to pay" by 129 percent.
[...]

[Nice article. Read it in its entirety. PGN]
<http://www.wired.com/wired/archive/10.11/start.html?pg=9>

✶ Re: BBC News: Fake bank website cons victims (Leeson, [RISKS-22.34](#))

<Hal Murray>
Tue, 05 Nov 2002 02:44:33 -0800

The PayPal scam mentioned in [RISKS 22.34](#) was relatively recent.

The technology was developed several years ago on AOL. It was common enough that it inspired the coining of a new term - phishing (for passwords and/or credit card numbers). The part I know about was mostly used by spammers. With a password, they could use the victims AOL account to send spam. With a credit card, they could sign up for more throw-away dial-up accounts to use for spamming.

Feed aolbilling to google-groups for more than you want to know: aolbilling.com is currently registered to somebody in Korea.

Here is a URL from May, 2000 describing the second wave - Yahoo, Hotmail...

<http://news.com.com/2100-1023-240295.html?legacy=cnet&tag=st.ne.ron.lthd.ni>

✉ Re: Windows daylight saving and file time-stamp (Jakeman, [R-22.34](#))

Graham Mainwaring <graham@mhn.org>

Tue, 5 Nov 2002 15:22:27 -0500 (EST)

In [RISKS-22.34](#), Chris Jakeman reports that Windows "changes the time stamp on all of its files" when the local time is adjusted due to Daylight Savings Time. Windows does in fact get it wrong, but not in the way that Mr. Jakeman describes. Windows, like Unix, stores time stamps as GMT/UTC time. All file system transactions are performed using this internal representation. When times are displayed to the user, they are reported in the currently applicable local time, as adjusted. When the time change occurs, there are no retroactive changes made to the contents of the filesystem.

The nature of the error is this: On most Unix variants, when a GMT time value is formatted for display to the user, the locale or timezone files are consulted to determine whether DST was in effect at the time in question. So a file that was created at 5:00pm (US) EST on March 1st, 2002 will always be reported as 5:00pm. Windows, on the other hand, appears to calculate whether DST is applicable **right now** and apply this offset to all dates indiscriminately. So a file created at 5:00pm EST on March 1st, 2002 will say "5:00pm" until the time change occurs on April 7. After that, the one-hour offset is applied, so this file is now reported to have been

created at 6:00pm EDT. Which is sort of technically correct: If you interpret "EDT" to be a permanent timezone that is offset by one hour, and the time change as a movement of a region between EST and EDT, then reporting the time as "6:00pm EDT" is not actually wrong. It is, however, very misleading.

The lesson to be learned is that if you are doing any sort of date comparison, date processing, etc., you really want to compare GMT to GMT times, not local to local times. If you do all internal processing in GMT then you don't have to know or care what time zone all your users are located in. If Mr. Jakeman's replication software had made its comparisons this way, it would have behaved correctly.

Also note that this specific problem's first mention in RISKS (as far as I can determine) was in [RISKS-6.55](#) (April 1988) as "Yet Another UnTimely Risk." The tone of the article was woeful that software engineers had continued to fail to implement correct solutions to this well-known problem - and that was more than fourteen years ago. There is also an interesting reference in [RISKS-6.70](#) to what I assume was the forerunner of the Gnu libc6 locale system.

✶ Re: Risks of dual-boot systems (Schreiber, [RISKS-22.34](#))

"Scott Nicol" <snicol@apk.net>

Mon, 4 Nov 2002 21:53:49 -0500

This is a well-known problem, and it seems to crop up in risks twice a year. Windows 98 stores the local time, Windows 2000 stores GMT and calculates the offset to the current time. Windows 98 is the real culprit here. Windows NT/2000/XP do the right thing, as does unix. I have no idea what older MacOS versions do, but I assume OS X does the right thing, too.

Hopefully in a few more years, Windows 98 (also 95 and me) will be dead and buried.

[In a response to Graham Mainwaring's item above, Scott also noted that "Up until about 5 years ago, RCS and CVS got this wrong." John Trammell said he would not blame this on dual-boot systems. "Perhaps a better description of the problem is 'not playing well with others,' or more simply, not following the Golden Rule. PGN]

✶ Re: Risks of dual-boot systems (Schreiber, [RISKS-22.34](#))

Tony Finch <dot@dotat.at>
Tue, 05 Nov 2002 03:24:36 +0000

It's good to see that the old jokes are still the best.

RISKS items on this specific summer time problem include (numbers are volume.issue.subject.item from the catless/risks.org archive):

[18.3.2.1](#)

[18.96.3.1](#)

[19.6.9.1](#)

[19.11.6.1](#)

[19.12.14.1](#)

[19.64.7.1](#)

Hilarious. There are at least ten times as many other RISKS articles on other summer time problems, if you're after more laughs. I think I'd bust a gut if I listed them all here! My favourite variation on this theme is the Windows 95 bug that would set the clock back when summer time ended, then again an hour later (because that's when summer time ends), and again an hour later... Who needs to reboot into another OS? What a pity that planned obsolescence deprives us of such entertainment!

Tony. f.a.n.finch <dot@dotat.at> <http://dotat.at/>

✶ Re: Risks of dual-boot systems (Schreiber, [RISKS-22.34](#))

Colin Andrew Percival <cperciva@sfu.ca>

Tue, 5 Nov 2002 05:43:08 -0800 (PST)

The problem of adjusting for DST twice is not restricted to dual-boot systems. Last year, my computer (running windows 2000) adjusted itself automatically from 2AM to 1AM; I rebooted it at roughly 1:30AM; and half an hour later it adjusted itself back to 1AM again. One imagines that if a "Reboot" task was scheduled for 1:30AM, the machine might cycle indefinitely.

While this particular bug has hopefully been fixed by now, the multitude of DST-related problems suggests that using UTC (or, even better, TAI) internally and treating DST (and leap seconds) as time zones -- restricted to user interface purposes only -- would be a much better solution.

✶ Re: Risks of dual-boot systems

Nick Rothwell <nick@cassiel.com>
5 Nov 2002 13:50:47 -0000

This is an old problem - we first encountered it about five years ago when we started building dual-boot Linux/Windows boxes. The only sensible approach to daylight-savings on such systems is to keep the hardware clock on UTC and let the operating systems maintain their own local offsets. Windows systems have, as far as I know, never had this option (perhaps to discourage users from dual-booting into a competing operating system?).

I allow Linux to do the Right Thing (hardware UTC, software adjustment) and when I need to boot into Windows during the summer I just disable the taskbar clock and use my wristwatch.

nick rothwell -- composition, systems, performance -- <http://www.cassiel.com>

✶ Re: Risks of dual-boot systems (Schreiber, [RISKS-22.34](#))

David Crooke <dave@convio.com>
Mon, 04 Nov 2002 19:34:41 -0600

I'd be interested to know the justification for using a dual-boot PC for a mission critical *anything*. Personally I wouldn't use Windows at all, far less a system that isn't even active some of the time, subject to the whims of a user.

It's yet another example of legacy functionality (MS-DOS requires the hardware clock to be in current local time as it has no timezone support, so DOS-based Windows has a workaround, ...) propagating for years and years into unrelated and inappropriate environments (Win 3.x -> Win 9x -> NT -> NT5).

✶ Wireless networking and security: CERIAS/Accenture roundtable

Gene Spafford <spaf@cerias.purdue.edu>
Mon, 4 Nov 2002 09:48:11 -0500

In May 2002, CERIAS and Accenture convened a roundtable of experts on wireless networking and security. The group met for 2 days to discuss the security challenges associated with wireless networking. The results of that roundtable discussion are now available online.

<http://www.cerias.purdue.edu/securitytrends/>

for the full report, executive summary, and "best practices" document.

REVIEW: "Internet Security Dictionary", Vir V. Phoha

Rob Slade <rslade@sprint.ca>

Tue, 5 Nov 2002 08:00:52 -0800

BKINSCDC.RVW 20020824

"Internet Security Dictionary", Vir V. Phoha, 2002, 0-387-95261-6,

U\$39.95

%A Vir V. Phoha

%C 175 Fifth Ave., New York, NY 10010

%D 2002

%G 0-387-95261-6

%I Springer-Verlag

%O U\$39.95 212-460-1500 800-777-4643 mspano@springer-ny.com

%P 259 p. + CD-ROM

%T "Internet Security Dictionary"

There are a few decent computer dictionaries extant, and at least a half dozen really good communications dictionaries among the many that have been published. However, until this, there was no security dictionary available in printed form, and there has been a need for one. (In fact, I've been working on one for a while, so, boring as it may be, I have to declare yet another possible conflict of interest.)

There are 1,400 terms defined, but a number are simply minor variations on a theme. (There are, for example, twelve phrases beginning with

"access.")

Much of the material is based the old US military terminology from the (now, generally) superseded "Rainbow series" (which is listed), and so there are a number of traditional but obsolete expressions. Some new and slang terms have been included, but some of these are only very vaguely related to the security topic. (The phrase "ankle-biter" is defined as a synonym for "script kiddie," but this term is generally used for a young, or inexperienced, neophyte in any technical field, and doesn't have a specific meaning in security.) Definitions tend to be terse, and may lack necessary detail. (The definition of "Chernobyl packet" seems to fit a smurf attack [also listed], but, due to the lack of information, it is impossible to tell.) An attempt has been made to make sure the material is up to date: Carnivore is listed (but not wardialling or wadriving). (The definitions for virus and worm are, as usual, unfortunate.)

Overall, despite the problems, this is a useful reference. Primarily, of course, this is because it is the first of its type. However, it does cover a reasonable range of the security field, and is, for the most part, reliable within limits. However, I would hope that the content is updated, expanded, and improved relatively soon, and regularly thereafter.

copyright Robert M. Slade, 2002 BKINSCDC.RVW 20020824
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

<http://victoria.tc.ca/techrev/~rslade> or <http://sun.soci.niu.edu/>

✦ Digital System Design DSD 2003 cfp

Henry Selvaraj <selvaraj@unlv.edu>

Fri, 01 Nov 2002 11:35:59 -0800

DSD 2003: EUROMICRO SYMPOSIUM ON DIGITAL SYSTEM DESIGN

Architectures, Methods and Tools

Antalya, Turkey, September 3-5, 2003

Submission date for papers: 3 Mar 2003

<http://www.egr.unlv.edu/~selvaraj/dsd03>

The Symposium on Digital System Design addresses architectures and implementations of (embedded) digital systems, as well as efficient design methods and tools. It is a premier discussion forum for researchers and engineers working on state-of-the-art investigations, development, and applications of digital systems, processor and memory architectures, application specific processors, systems-on-a-chip, hardware/software co-design, circuit design, system validation, and design automation.

The main areas of interest are Processor and memory architectures; Special architectures; Specification and modeling; Validation; Synthesis; Systems-on-a-chip; Applications of (embedded) digital systems
[PGN-ed]



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

[ACM](#) Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 36

Thursday 7 November 2002

Contents

- [CNN needs some fact-checkers on electronic-election article](#)
[Rebecca Mercuri](#)
- [The 2002 general election](#)
[PGN](#)
- [Dominant lottery vendor cracked](#)
[Conrad Heiney](#)
- [Winning lottery tickets can be determined before purchase](#)
[Jeremy Epstein](#)
- [Robot malpractice?](#)
[Paul Saffo](#)
- [Computer problem caused fatal pipeline rupture](#)
[Paul Hirose](#)
- [Opera confused about hemispheres](#)
[David Skillicorn](#)
- [Set your clock to 1984](#)
[Toby Gottfried](#)
- [Scoping out the future](#)
[NewsScan](#)
- ['British' spelling](#)
[Michael Bacon](#)

- [NSF Trusted Computing Program](#)
[Carl E. Landwehr](#)
 - [REVIEW: "The Total CISSP Exam Prep Book", Peltier/Howard](#)
[Rob Slade](#)
 - [REVIEW: "Information Security", Donald L. Pipkin](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✂ CNN needs some fact-checkers on electronic-election article

"Rebecca Mercuri" <notable@mindspring.com>

Wed, 6 Nov 2002 08:59:29 -0500

The 5 Nov 2002 article "Electronic elections: What about security?"

(www.cnn.com/2002/TECH/ptech/11/05/touch.screen/index.html) on CNN.com by

Jeordan Legon contains a number of factual errors and misrepresentations. To CNN's credit, they did attempt to contact me for an interview on 11/4 for that article, but their tight deadline should be no excuse for not getting the facts straight.

The article states: "the voting software and hardware has to pass strict security standards imposed by the Federal Election Commission and the National Association of State Election Directors." This is untrue. ALL voting systems newly deployed for the 2002 election were inspected to the OBSOLETE 1990 FEC recommendations. Even these were only adopted by 2/3 of the States. The 2002 standards must be adopted prior to use and it is unclear when (or in some States if) this will happen.

Mark Beckstrand, a Sequoia Voting Systems VP, was quoted in the CNN article as saying: "Show me somebody who has gotten into our software. We haven't lost or misplaced or ever been accused of not having 100 percent accuracy." Well, first of all, experts, such as myself, are prevented from looking at Sequoia's equipment because it is sold under restrictive trade-secret agreements making it a felony if a purchaser (such as a County Board of Elections) provides it for internal inspection, except under court order. For a court case in Palm Beach County, we have tried for months to obtain a Sequoia machine (for which we have numerous affidavits from voters indicating problems) in order to perform an internal inspection, and have even offered to purchase a machine from the County outright, but so far have been barred from doing so. It makes it really hard to show if their product has been tampered with, if it's a felony to inspect it.

In addition to our case in Boca Raton, where there was an 8% "undervote" (votes missing compared with number of voters who signed in at the election), there are other instances of problems involving Sequoia equipment. Susan Bernicker videotaped numerous Sequoia machines used in a Louisiana election that showed different names on the confirmation screen than the candidate buttons that were pressed. Over in New Jersey in 2000, a brand new Sequoia machine turned up zeros for some candidates in a local election. Elsewhere in Palm Beach Co. in March 2002, Sequoia systems

registered a 3% undervote in an election where only 2 candidates were running in only 1 race. It was conjectured (by Election Supervisor Theresa LePore) that people came to the polls and deliberately did not vote for one of the candidates, but this seems rather unlikely.

Sequoia seems to have a short memory when it comes to court cases and missing votes. There might be a good reason for this. According to the San Francisco Business Times (11/19/2001), their Southern Regional Sales Manager, Phil Foster, was indicted in Louisiana for "conspiracy to commit money laundering and malfeasance" involving kickbacks to Jerry Fowler, the Louisiana state commissioner of elections, now serving a prison term for his involvement in a decade-long kickback scheme with Sequoia. Foster sold machines in Louisiana and Florida, and testified as a technical expert against Bernicker in her Baton Rouge case.

I hope CNN can be encouraged to run a correction or follow-up on their article. The public needs to know the rest of this story.

⚡ The 2002 general election

"Peter G. Neumann" <neumann@csl.sri.com>
Wed, 6 Nov 2002 9:38:58 PST

In yesterday's voting, there were numerous irregularities, as usual -- although perhaps fewer visible ones than had been anticipated.

* Palm Beach and Broward in FL had reports of voters touching the screen for McBride and having the vote showing up for Bush. The vendors and voting officials claim that that error was quickly "fixed". Remember that "fix" has two meanings. For example, check out the Matt Drudge report at

<http://www.drudgereport.com/>

<http://www.drudgereport.com/vote1.htm>

* In Broward County, a programming error left out 34,000 votes, because the combination of early votes exceeded a preprogrammed maximum. Also, 70,000 absentee and Spanish-language ballots were missing from the reported turnout, although they were included in the vote totals. These were later corrected.

* In Houston, where the all-electronic voting machines have rotary dials instead of touch-screens, voters in five precincts had their attempts to vote a straight party ticket rejected. (It happens to have been the Democratic ticket that was not accepted.)

* In Georgia, newly using touch-screens, some voters reported their votes being recorded for other candidates.

* In Pulaski County, Arkansas, half of the voters had not been assigned precincts after redistricting and were denied being able to vote despite having legitimate registration cards.

* San Francisco failed to deliver enough ballots to several precincts, where voting continued until midnight.

* In Nebraska, Charlie Matulka (a long-shot Democratic candidate) reports having been given a paper ballot already premarked for his Republican opponent.

* In South Carolina, there were some reports of long waits in line. Elsewhere, people turned away from the polls in various places even with valid identification. Also, reports of lever machines dropping votes.

NOTE: Andrew Klossner sent in a correction on Andrew Morton's item in [RISKS-22.35](#) on absentee voting in Oregon: the ballot he gets is just an unlabeled punch-card in which he has to punch out the chad for the desired holes. (Same for me in Santa Clara County, California. PGN)

The general consensus among election officials and voters seems to be that the all-electronic machines are a great improvement, relatively easy to use, and inherently able to prevent overvotes. The general consensus among knowledgeable computer security experts seems to be that almost all of the existing all-electronic systems could relatively easily be rigged by internal fraud in the software and external manipulation of the local polling-place configurations and could also be subject to undetected internal errors, because of an almost complete absence of meaningful audit trails and independent verification of the consistency of votes tabulated with votes cast. Just because an all-electronic machine looks like it might be working, how do you *KNOW* it is doing the right thing? From a RISKS

perspective, a perceived potential lack of integrity is a serious obstacle to democracy.

✶ Dominant lottery vendor cracked

"Conrad Heiney" <conrad@fringehead.org>

Wed, 6 Nov 2002 10:45:47 -0800

According to the **Wall Street Journal**, 6 Nov 2002, the world's dominant operator of national and state lotteries has warned of a possible compromise of its system for patching scratch-ticket winners. The company referred to an "operational and technical issue" in which the bar code used on the ticket had been cracked. The article quotes an unnamed source who claims someone had "decoded the algorithm" for the bar codes.

Setting aside the RISK of whichever algorithm they chose, and not knowing whether this was an inside job, it's interesting to contemplate what other technology based industries have become so thoroughly centralized that one crack can cause a worldwide mess like this.

http://online.wsj.com/article/0,,SB1036548523995761668,00.html?mod=3Dhome_whats_news_us

http://online.wsj.com/article/0,,SB1036548523995761668,00.html?mod=3Dhome_whats_news_us

Conrad Heiney <conrad@fringehead.org> <http://fringehead.org>

✶ Winning lottery tickets can be determined before purchase

"Jeremy Epstein" <jepstein@webmethods.com>

Wed, 6 Nov 2002 17:14:40 -0500

According to <http://money.cnn.com/2002/11/06/technology/gtech/index.htm>,

GTech (the largest lottery operator) has determined that the scratch-off

lottery tickets can be determined before doing the scratch-off operation.

"A corrupt ticket salesperson that knew the codes theoretically could pick

out the winners on a sheet of tickets and cash them, selling only the losers

to the general public."

Sounds like the serial/code number isn't being encrypted or otherwise

protected before being printed...

✶ Robot malpractice...

Paul Saffo <psaffo@iftf.org>

Wed, 06 Nov 2002 20:30:16 -0800

http://www.sptimes.com/2002/10/30/TampaBay/Patient_dies_in_robot.shtml

In an surgical operation to remove a cancerous kidney at St. Joseph's

Hospital in St Petersburg, a three-armed da Vinci robot (made by Intuitive

Surgical Inc.) was being controlled by an experienced doctor from a

3-dimensional computer screen, 10 feet away. The robot

technology for cutting blood vessels is supposed to decrease bleeding, pain, and recovery time. Unfortunately, the patient's aorta and another blood vessel were cut, and this went unnoticed for an hour and one-half. Two days later, the patient died of complications. The developer found no mechanical problems, and absolved the robot, which had been used successfully in 10 similar operations. [Source: Patient dies in robot-aided surgery; Such robots are considered a major surgical breakthrough, but something went wrong, Graham Brink, *St. Petersburg Times*, 30 Oct 2002; PGN-ed]

[Classical case. The vendor absolves the technology, implicating the doctor. Others blame the robot. What about the doctor-machine interface?
PGN]

✶ Computer problem caused fatal pipeline rupture

Paul Hirose <pshirose@earthlink.net>
Wed, 06 Nov 2002 06:43:40 GMT

The NTSB (U.S. National Transportation Safety Board) has released its report on the pipeline accident at Bellingham, Washington, in June 1999. Three people were killed when a 16-inch pipeline ruptured and released about 237,000 gallons of gasoline, which then ignited.

One link in the chain of events leading to this accident was the pipeline company's SCADA (supervisory control and data acquisition)

system. Just before the rupture, there was a pressure surge in the pipeline. This was a common occurrence, unrelated to the SCADA. But through rotten luck the surge hit right in the middle of an extreme slowdown in the SCADA computer. Since the SCADA controlled the pumps and valves along the pipeline, the control room operator was unable to relieve the pressure. Had the computer responded promptly to his commands, pressure probably would have remained within the pipeline's burst strength.

A pair of DEC VAX computers (one active, one standby) ran the SCADA software. Investigators attempted to duplicate the system slowdown but were not successful. Nor were any flaws uncovered in the hardware or software. However, there were flaws in the company's computer procedures.

1. All computer operators used the same login. The account had system administrator privileges, including unlimited authority to hog resources.
2. Modifications to the SCADA historical database were performed on the same computer that was in control of the pipeline. Just before the SCADA became unresponsive, the system administrator had added some database records. That probably triggered the SCADA lockup, concludes the NTSB report.
3. Although the system administrator monitored error logs to check the progress of his database work, and began to see errors 18 minutes before the rupture, he did not warn the pipeline control room or his supervisor. Instead, he left the computer room for about 15 minutes.

4. Anyone with an account could log in to the SCADA through a dialup connection. However, the fact that the system troubles began shortly after the database modification, and stopped when the new records were deleted, suggested that an intruder was not to blame.

In the wake of the accident, the pipeline company rectified these problems.

Executive summary and complete accident report are on line:
<http://www.nts.gov/publicctn/2002/PAR0202.htm>

✶ Opera confused about hemispheres

David Skillicorn <skill@it.uts.edu.au>

Thu, 07 Nov 2002 08:54:44 +1100

This morning (local time), the web browser Opera is serving Australians with banner ads intended for Austria.

The relatively small difference in syllables has been the cause of much misdirected physical mail over the years (puzzling to the Austrians who spell their country completely differently). Now the small difference between .au and .at seems to be causing the same problems in the cyberworld.

✶ Set your clock to 1984

"Toby Gottfried" <toby@gottfriedville.net>

Wed, 6 Nov 2002 11:17:32 -0800

Along the lines of the FBI-bugs-libraries reference in RISKS
22:35

<http://catless.ncl.ac.uk/Risks/22.35.html#subj3>

there is also this article about cooperation between ISPs and
the prying

eyes of government on e-mail.

<http://www.thenation.com/docprint.mhtml?>

[i=20021111&s=mejia20021030](http://www.thenation.com/docprint.mhtml?i=20021111&s=mejia20021030)

Looks like Orwell should have called his book "2004".

✶ Scoping out the future

"NewsScan" <newsscan@newsscan.com>

Thu, 07 Nov 2002 09:26:47 -0700

Yale computer scientist David Gelernter is glad that the
Microsoft trial is
behind us, because "operating systems are lapsing into senile
irrelevance,"

and we need to move on to the future. And what will the future
be all about?

"Every piece of digital information you own or share will appear
(in the

near future) in one universal structure" -- one to which you'll
have access

from any Net-connected computer anywhere. "I have time for only
one screen

in my life," says Gelernter. "That screen had better give me
access to

everything, everywhere." The universal structure, dubbed
Scopeware, will be

a narrative, 3D stream of electronic documents flowing through
time. "The

future (where you store your calendar, reminders, plans) flows into the present (where you keep material you're working on right now) and on into the past (where every e-mail message and draft, digital photo, application, virtual Rolodex card, video and audio clip and Web bookmark is stored, in addition to all those calendar notes and reminders that used to be part of the future and have since flowed into the past to be archived forever)."

[*The New York Times*, 7 Nov 2002; NewsScan Daily, 7 November 2002]

<http://partners.nytimes.com/2002/11/07/technology/circuits/07soft.html>

^'British' spelling (in "Software leaves ..., [RISKS-22.35](#))

"Michael \ (Streaky\) Bacon" <streaky.bacon@easynet.co.uk>

Wed, 6 Nov 2002 06:48:00 -0000

PGN, The RISK here is that of assuming 'British' spelling exists -- it is the Oxford ENGLISH Dictionary for spelling and the Queen's ENGLISH for pronunciation. <GRIN>

Simply put, Britain comprises the 'home countries' of England, Northern Ireland, Scotland and Wales. There are other island territories immediately offshore that are part of Britain (eg. the Scilly Isles) and others that are part of the United Kingdom but not of Britain (e.g., the Channel Islands).

[LATER CORRECTION: Northern Ireland is NOT a part of Great

Britain,

but is a part of The United Kingdom of Great Britain and Northern Ireland,

as of 1927. Thanks to John Carlyle-Clarke for this fact! PGN]

There is no 'British' language per se -- the (recent -- i.e., immediately pre-AD) native majority tongues of Great Britain were basically Celtic, French and Latin (by today's definitions) -- English arose as a combination of these and other, imported, languages. Today, basically, the native Welsh language is Celtic, the native Scots language is Celtic, the native Irish language is Celtic, and the native English language is English -- except for Cornwall (a county) where their native language is Celtic. The individual country variation of the Celtic language is frequently spoken in Wales and in the Highlands of Scotland (and in Cornwall).

I was raised in Jersey (the Channel Island, not the State). This is part of the United Kingdom, but not the European Union (confusing isn't it?) where I grew up speaking 'Jersey patois' (a form of Norman French) and English.

So. 'English spelling' - yes, 'British spelling' - no. With "tongue" slightly in cheek, Michael (Streaky) Bacon

NSF Trusted Computing Program

"Landwehr, Carl E." <clandweh@nsf.gov>

Tue, 5 Nov 2002 17:57:47 -0500

The next proposal deadline for NSF's continuing Trusted

Computing program is
Wednesday, December 4, 2002. Links to the program announcement,
as well as
a summary description and list of the initial awards under NSF's
Trusted
Computing program can be found on NSF's web. NSF has changed
its Web
infrastructure recently, so the direct URL for the Trusted
Computing Program
is a bit lengthy:

[http://www.cise.nsf.gov/div/ccr/fndg/display.cfm?
pgm_pims_id=5158&pgm_supp_id=10091&loc=ccr&pub_id=5370](http://www.cise.nsf.gov/div/ccr/fndg/display.cfm?pgm_pims_id=5158&pgm_supp_id=10091&loc=ccr&pub_id=5370)

[http://www.cise.nsf.gov/div/ccr/fndg/display.cfm
?pgm_pims_id=5158&pgm_supp_id=10091&loc=ccr&pub_id=5370 \[split\]](http://www.cise.nsf.gov/div/ccr/fndg/display.cfm?pgm_pims_id=5158&pgm_supp_id=10091&loc=ccr&pub_id=5370)

Alternatively you can visit:

www.cise.nsf.gov

and then select "funding opportunities" and then select "trusted
computing".

If you are in a position to conduct research in this area, I
encourage you
to consider submitting a proposal this year. NSF focuses on
funding research
at universities and not-for-profit organizations. I also hope
you will
consider helping me staff the review panels for the proposals
that are
submitted. My warm thanks to all who proposed and who
participated in the
review process this past year.

Carl Landwehr, Director, Trusted Computing Program clandweh@nsf.gov
National Science Foundation 1-703-292-8936

🔥 REVIEW: "The Total CISSP Exam Prep Book", Peltier/Howard

Rob Slade <rslade@sprint.ca>

Wed, 6 Nov 2002 04:34:19 -0800

BKTCIEPB.RVW 20020823

"The Total CISSP Exam Prep Book", Thomas R. Peltier/Patrick D. Howard,

2002, 0-8493-1350-3, U\$59.95

%A Thomas R. Peltier

%A Patrick D. Howard

%C 920 Mercer Street, Windsor, ON N9A 7C2

%D 2002

%G 0-8493-1350-3

%I Auerbach Publications

%O U\$59.95 800-950-1216 auerbach@wgl.com orders@crcpress.com

%P 287 p.

%T "The Total CISSP Exam Prep Book: Practice Questions, Answers, and

Test Taking Tips and Techniques"

Both the preface and the back cover copy stress the assertion that "until now, [CISSP (Certified Information Systems Security Professional) candidates] were not afforded the luxury of studying a single, easy-to-use manual." Despite the reservations that I may have about the quality of their works, this statement must surely be a shock to Shon Harris (cf. BKCISPA1.RVW), Mandy Andress (cf. BKCISPEC.RVW), S. Rao Vallabhaneni (cf. BKCISPET.RVW), and Ronald Krutz and Russell Vines (cf. BKCISPPG.RVW) and Carl Endorf (wait for it). (Well, I suppose that, technically, Vallabhaneni's is *two* books ...)

It would be difficult to say that you could use this volume for study, either. It doesn't actually have any tutorial material, other than some advice on how to write the exam. Some of the tips are outdated,

and most of the rest of the content is rather generic, such as the suggestion to eat a hearty breakfast before you go. (I'd suggest that you go easy on the recommendation to drink lots of coffee before you head off: some of the proctors can be pretty sticky about letting you go to the washroom.)

What it does have is ten chapters (one for each of the CBK [Common Body of Knowledge] domains) of twenty five "exam" questions each. That's twenty five questions for physical security (the smallest domain) and twenty five questions for telecommunications (the largest). The questions in the chapters have explanations of which answers are right and which are wrong. Then there is a sample "exam," and then the same exam with the answers.

Sample exams are highly sought after: it makes sense to know the type and style of questions that you may encounter on the exam. There is only one problem: (ISC)² doesn't hand out sample exams. In fact, they guard the exam questions rather closely. The sample exams at ccure.org are a staple in CISSP study groups, and there is a commercial outfit that will sell you a set that they have made up.

Essentially, of course, this is what Peltier et al. have done. So, the question is, how close are the sample questions in this book to the real thing.

The answer, unfortunately, is not very. Different people worked on the

questions for different chapters, so the level of success varies. (Security management has possibilities, telecommunications is rather ghastly.) Ultimately, though, these questions are not representative of what you will find on an actual CISSP exam. Those familiar with Bloom's Taxonomy of questions will know that you progress from simple questions of fact through synthesis of multiple facts through analysis based on synthesis to a level of judgment or critical thinking. Most of the questions a candidate will encounter on the CISSP exam are at the analytical or critical levels. Too many of the questions found in most sample exams are at the simple factual level. The questions in this current work do move beyond the simplistic, but they tend to turn on specific wording in some very weak references, rather than the principles and concepts encountered in the CISSP exam itself. (Appendix A is a bibliography used in the creation of the questions, and it is a decidedly poor one.) Some questions and answers are flatly wrong (planting malicious software is definitely **not** a passive attack). Others may have some point to their creation but get confused. One question states that a certain answer is not correct because the technology is not an encryption algorithm, but the "correct" answer isn't an algorithm either.

This book may give you a very rough idea of the types of questions you may encounter, and the range of topics you may need to know. If you rely on it to prepare you for the exam, however, you may be in for a rude

shock.

copyright Robert M. Slade, CISSP, 2002 BKTCEPB.RVW 20020823
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com
<http://victoria.tc.ca/techrev/~rslade> or <http://sun.soci.niu.edu/~rslade>

REVIEW: "Information Security", Donald L. Pipkin

Rob Slade <rslade@sprint.ca>
Thu, 7 Nov 2002 07:45:52 -0800

BKISPTGE.RVW 20020823

"Information Security", Donald L. Pipkin, 2000, 0-13-017323-1,
U\$39.99/C\$60.00
%A Donald L. Pipkin
%C One Lake St., Upper Saddle River, NJ 07458
%D 2000
%G 0-13-017323-1
%I Prentice Hall
%O U\$39.99/C\$60.00 +1-201-236-7139 fax: +1-201-236-7131
%P 364 p.
%T "Information Security: Protecting the Global Enterprise"

It takes quite a while to figure out what Pipkin is trying to do in this book. Ultimately, there is coverage of some of the important basic concepts involved in information security. However, the text as a whole is both confused and confusing.

The prologue tells us that business is changing and chaotic, and that information is of prime importance. The introduction takes a quick run

through a few of the basic security concepts, with an emphasis on business continuity planning.

Phase one of the book is entitled "Inspection," but the prologue lists some items of concern in risk analysis. Chapter one, called "Resource Inventory," is concerned with data classification. It touches on, but does not really discuss, the orthogonal nature of classification schemes when confidentiality, availability, and integrity must be considered. The material is sparse, and, while there are some indications of forward references to later chapters, those chapters do not get down to practical details either. Chapters two to six begin to examine the concepts of threats (concentrating, very poorly, on malicious software), loss analysis (many examples, little of substance), vulnerabilities, safeguards, and assessment.

Phase two, on protection, seems to be trying to expand chapter five, but really just repeats prior material. Concepts touched on include access, identification, authentication, authorization, and accountability. Mixed in are the not-quite-related topics of availability, accuracy, confidentiality, and administration.

Phase three looks at intrusion detection, with chapters on intrusion types, methods, process, and detection methods. It isn't very useful.

Phase four reviews incident response, but rather vaguely.

Phase five concerns the post-mortem reflection. The chapter on documentation has some useful material on the contents of after-

action

reports, but the rest of the content is unfocused and generic.

It is not quite true to say that the book is unstructured: it has a structure, but either does not follow it, or does not usefully employ it.

Those without a security background will find it hard to build a useful or

working framework from the material in this book. Those with such a

background will eventually find that the parts of the book do fit neatly, if

not logically, into the common framework. However, those with such a

background will have no need for this work.

copyright Robert M. Slade, 2002 BKISPTGE.RVW 20020823

rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca

pl@canada.com

<http://victoria.tc.ca/techrev> or <http://sun.soci.niu.edu/~rslade>



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

[ACM](#) Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 37

Saturday 9 November 2002

Contents

- [Lynn Landes' analysis of the 2002 Elections](#)
[PGN](#)
- [Quote on election integrity](#)
[Susan Marie Weber](#)
- [Georgia election memory-card problem](#)
[Lillie Coney](#)
- [Unsupervised biometric scanners more toys than serious security measures](#)
[c't via Markus Kuhn](#)
- [U.S. Navy sites spring security leaks](#)
[Lillie Coney](#)
- [Internet home banking unsafe](#)
[Erling Kristiansen](#)
- [Driver killed in "computer-controlled" AirTrain](#)
[Daniel Norton](#)
- [Man banned from driving after trusting in-car computer](#)
[Matthew Bloch](#)
- [Small things add up](#)
[Bill Lamb](#)
- [Re: 'British' spelling](#)
[Christopher Allen](#)

- [Re: What if ... the pundits had nothing ...](#)
[Edward Reid](#)
 - [REVIEW: "Information Assurance", Joseph G. Boyce/Dan W. Jennings](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ **Lynn Landes' analysis of the 2002 Elections**

"Peter G. Neumann" <neumann@csl.sri.com>

Fri, 8 Nov 2002 11:30:35 PST

[This item is included in its entirety with the permission of the author.]

2002 Elections: Republican Voting Machines,
Election Irregularities, and "Way-Off" Polling Results
By Lynn Landes, 8 Nov 2002

"The Republicans will never give up their voting machines," said a top Republican party official to Charlie Matulka, the Democratic candidate for the U.S. Senate seat in Nebraska. This statement was in response to Charlie's very public protest against the conflict-of-interest inherent in the candidacy of Senator Chuck Hagel (R-NE). Hagel has held top executive positions (and still has investments) in companies that owned the machines that counted the vote in Nebraska this election and last.

Republicans dominate the voting machine business. So, I expected the Republicans to take back the Senate... amid reports of voting machine "irregularities" in several states and polling results that didn't come close to election outcomes. And with billions of dollars at

stake, who
could resist the temptation to tweak results? It's duck soup.

Dr. Rebecca Mercuri, the nation's leading expert in voting machine technology, says, "Any programmer can write code that displays one thing on a screen, records something else, and prints yet another result." But they do make mistakes as we know from the multitude of reports in this election and past ones. Dr. Mercuri's real fear is that one day the "irregularities" will go away, as programmers learn their clandestine craft all too well.

Then how can we tell if the "fix was in?" An examination of exit polling and pre-election polling versus election results could raise a few red flags.

We can't use Voter News Service (VNS) this year. VNS is a top-secret private consortium owned by ABC News, The Associated Press, CBS News, CNN, Fox News, and NBC News that has "projected" election night winners since 1964. VNS collapsed camp on election day due to technical problems... they said. Or was it the glare of publicity since the 2000 presidential election that brought the charade to an end? Questions have been raised since its inception, that VNS was a cover for election day vote rigging or other shenanigans. And it was strange that when VNS management made its announcement on Tuesday, they didn't make a big deal over how the shutdown affected the 64,000 temporary employees they claim they hired for this election.

Anyway, that leaves us with pre-election polling to ponder. An intensive effort to review and interpret that data is currently underway by Bev Harris and her staff at Talion.com.

Meanwhile, I called John Zogby of the highly respected Zogby International. I asked him if over the years he had noticed increased variation between pre-election predictions and election results. Zogby said that he didn't notice any big problems until this year. Things were very different this time. "I blew Illinois. I blew Colorado (and Georgia). And never in my life did I get New Hampshire wrong...but I blew that too." Or did he?

This year might instead be a repeat of the 2000 presidential election, when the polls accurately predicted the winner (Gore), but the voting system in Florida collapsed under the weight of voting machine failure, election day chicanery, and outright disenfranchisement of thousands of black voters by Republican state officials.

And for those who believed that the new election reform law does anything to protect the security of your vote...think again. The federal standards to be developed and implemented as a result of the new law will be VOLUNTARY. What Congress really did was to throw \$2.65 billion dollars at the states, so that they could lavish it on a handful of private companies that are controlled by ultra-conservative Republicans, foreigners, and felons.

Let's take a moment to look back rather than forward. In the last several

decades the rich have gotten richer and the poor poorer. This is not a formula for a conservative groundswell. Yet both conservative Democrats and right wing Republicans have long enjoyed success at the polls. While, most of Europe still uses paper ballots, voting machines have been in America since 1889. The use of computers in voting technology began around 1964. Today, less than 2% of the American electorate use hand-counted paper ballots.

The question is...have elections in America been rigged to slowly, but surely shift power to the right? In the secretive world of voting machine companies, anything is possible.

The sad fact is that the legitimacy of government in the United States will remain in question as long as over 98% of the vote is tabulated by machines that can be easily rigged, impossible to audit, and owned by a handful of private companies. Until we get rid of those voting machines, democracy in America may be a distant memory.

Lynn Landes is a freelance journalist specializing in environment and election issues on www.EcoTalk.org. Lynn's been a radio show host, a regular commentator for a BBC radio program, and news reporter for DUTV in Philadelphia, PA.

Lynn Landes, 217 S. Jessup Street, Philadelphia, PA 19107
(215) 629-3553 / (215) 629-1446 (FAX) lynnlandes@earthlink.net]

[Lynn's writings often also run on alternative online media, such as

www.CommonDreams.com. She has a Web page for VotingSecurity at <http://www.ecotalk.org/VotingSecurity.htm> . PGN]

Quote on election integrity

"SusanMarieWeber" <susanmarieweber@earthlink.net>

Fri, 8 Nov 2002 23:13:36 -0800

The right to have the vote counted is infringed, and we have lost the

integrity of our voting system, when the ease with which ballots can be

manipulated is greater than the ease with which the manipulation can be

detected. (Kevin Craig, 2000) www.electionguardians.org

[See: Broward vote total short by 104,000 in reporting glitch, Evan S. Benn and Elena Cabral, *Miami Herald*, 7 Nov 2002, for more on

the Broward County bulleted item noted in [RISKS-22.36](#).]

<http://www.miami.com/mld/miamiherald/news/politics/4461857.htm>

Georgia election memory-card problem

Lillie Coney <lillie.coney@acm.org>

Fri, 08 Nov 2002 10:22:35 -0500

ELECTION 2002: 2,180 Fulton ballots found late, 67 memory cards misplaced, but shouldn't change results, by Ty Tagami and Duane Stanford, *Atlanta Journal Constitution*, 8 Nov 2002

Fulton County election officials said Thursday that memory cards from 67

electronic voting machines had been misplaced, so ballots cast on those machines were left out of previously announced vote totals. Fifty-six cards, containing 2,180 ballots, were located Thursday. Eleven memory cards still were missing Thursday evening. If the cards could not be found, the votes would be retrieved from the voting machines, election officials said. [Bibb and Glynn Counties each had one card missing after the initial vote count, but the cards were located and counted the next day.][PGN-Excerpted]

⚡ Unsupervised biometric scanners more toys than serious security measures

<Markus Kuhn>

Wed May 29, 2002 11:16:20 AM US/Pacific

An even more fatal blow to off-the-shelf *unsupervised* biometric identification products was given recently by three authors in an article in the well-respected German computer magazine c't:

Lisa Thalheim, Jan Krissler, Peter-Michael Ziegler:
Körperkontrolle --

Biometrische Zugangssicherungen auf die Probe gestellt. c't
11/2002,
Heise Verlag, ISSN 0724-8679, p 114-, 17 May 2002.

An online English translation is now available on
<http://heise.de/ct/english/02/11/114/>

The team tested:

* six products involving capacitive fingerprint scanners

(Biocentric Solutions, Cherry, Eutron, Siemens and Veridicom)

- * two optical (Cherry, Identix) fingerprint scanners
- * one thermal (IdentAlink FPS100U) fingerprint scanner (Atmel FCD4B14 sensor)
- * Authentacam by Panasonic
- * an iris scanner that is currently being marketed in the USA and is scheduled to enter the European market in the near future
- * FaceVACS- Logon, a technical solution for recognizing faces developed by the Dresdner Cognitec AG

The authors "were able, aided by comparatively simple means, to outwit all the systems tested" and concluded that "the products in the versions made available to us were more of the nature of toys than of serious security measures" and that "business should not treat the security needs of its customers quite so thoughtlessly".

It is worth stressing that none of the deception techniques used are really applicable in a **supervised** two-factor application, for example where a border control or social benefits officer watches someone using the finger or iris scanner in order to confirm the identity information stored in a presented smartcard. The relevance of these attacks to the discussion about the use of biometric features in a national identity infrastructure is unfortunately sometimes misrepresented. I am still convinced that both iris scanning and finger print recognition in a **supervised** scan can be made easily several orders of magnitude more reliable than human

photo/face
comparisons.

What currently marketed sensors lack is a really robust detection technique for whether the detected signal comes from live human tissue, and this still looks very much like an open research problem. Parts of suitable solutions might be:

- * tests of various involuntary reactions that require significant effort to simulate, for example, is the iris pattern deforming correctly when the pupils contract because of illumination?
- * test whether the body part is functional, i.e. can the fingerprint be detected from a finger that is typing fluently on a keyboard or can the pupil inside the contracting iris read text at the same time?
- * is it possible to build low-cost spectrographic cameras/scanners that can distinguish materials and tissues by using hundreds instead of just three (red/green/blue) wavelength bands, etc.

Markus G. Kuhn, Computer Laboratory, Univ. of Cambridge, UK
mkuhn at acm.org

✶ U.S. Navy sites spring security leaks

Lillie Coney <lillie.coney@acm.org>
Fri, 08 Nov 2002 11:48:24 -0500

A French group known as Kitettoa discovered that files on several Navy Web

sites and other sides running IBM's Lotus Domino software were easily accessible. Exposed information included hundreds of trouble tickets since 1989 for the Consolidated Automated Support System; a Naval Supply Systems Command site that enables Navy personnel to order commercial software and internally developed applications -- including records on who registered to use the system and their passwords. The Navy apparently does not feel the information thus compromised was particularly sensitive, but has reportedly taken some systems off the Net and tighter security controls in others.

[Source: Wired News, 6 Nov 2002; PGN-ed]

Lillie Coney, Public Policy Coordinator, U.S. Ass'n for Computing Machinery
Suite 510, 2120 L Street, NW, Washington, D.C. 20037 1-202-478-6124

Internet home banking unsafe

Erling Kristiansen <erling.kristiansen@xs4all.nl>

Fri, 08 Nov 2002 22:13:48 +0100

The 28 Oct 2002 edition on the programme "Netwerk" of the Dutch TV station NCRV ran an item on Internet home banking. The programme featured a person accessing his bank account via Internet, and another person with a laptop reading a clear-text transcript of the session.

The programme was not very technical, but two hints were given that helped

in finding out what was going on: The two persons "were colleagues" (in network terms: were on the same LAN), and the scenario was described as a "man in the middle" attack. I know from own experience that the Dutch home banking system uses a secure web session. A challenge-response authentication device ("token" or e.dentifier) is used to authenticate the user, but this is not relevant to this discussion.

Poking around a bit, I found several references to a vulnerability in Internet Explorer 5.0, 5.5 and 6.0. A good explanation can be found at

<http://www.thoughtcrime.org/ie-ssl-chain.txt>

I am not an expert in SSL and PKI and such matters. But, in brief, as I understand it, a certification Authority can delegate its authority to somebody else. This is designed to be safe, provided, of course, it is implemented properly. IE skips one step in its implementation of the procedure, essentially allowing somebody who can gain access to the data stream (e.g. by being on the same LAN or having access to a router somewhere along the path) to delegate the certification authority to himself. This, in turn gives the man-in-the-middle access to the data. I am sure this description is not precise, but I hope it catches the essence of the attack. Otherwise, please read the referenced article.

I had an e-mail conversation with somebody from the TV programme, who confirmed that "indeed, it is a problem in IE". They did not say this in the programme because "the problem is the responsibility of the banks, not

Microsoft". Apparently, their aim was to expose the banks.

A few thoughts:

It would seem that the problem affects not only home banking but any application using a secure web session. The exploit also highlights that security depends not only on good design, but also on proper implementation. You have to trust the software vendor. Do you??

SPECULATION MODE ON

Why is Microsoft reluctant to fix this bug that is present in 3 consecutive versions of IE? In view of the nature of it, it cannot be that difficult to fix.

Could it be that they do not want to fix it? Either because they want to exploit it themselves, or because somebody twisted their arm to provide a back door.

SPECULATION MODE OFF

It is, actually, a very well hidden back door that is not easily discovered unless you have access to the source code, or you know what you are looking for. I wonder how it was discovered.

⚡ Driver killed in "computer-controlled" AirTrain

"Daniel Norton" <Daniel@DanielNorton.net>

Fri, 8 Nov 2002 11:22:40 -0500

I wrote last year ([RISKS-21.82](#)) about my concerns of a computer-controlled train (the JFK AirTrain) being installed that would carry hundreds of

passengers at speeds of over 60 miles per hour (95 kmh).

A test run of the system on 27 Sep 2002 was under manual control with automatic speed regulators deliberately disabled. The train was traveling about 55 miles per hour (90 kmh) when it approached a downhill curve, jumped the track, knocked away 150 feet (45m) of a concrete wall, and tore a gash in the front of the train. Tons of concrete in the train -- used as ballast to simulate passengers -- slid along the floor and crushed the driver to death.

As several pointed out in follow-ups to my post last year, the greater RISKS of train systems are human errors, and this recent tragedy seems to support that position.

[Of course, in the JFK train test, the driver was posthumously blamed for going to fast. Perhaps that was the speed they had asked him to reach, as part of the test? And who is to blame for not realizing that the ballast should have been anchored down? So, that's what testing is for? A substitute for thoughtful design and operation? PGN]

✶ Man banned from driving after trusting in-car computer

Matthew Bloch <matthew@bytemark.co.uk>

Sat, 9 Nov 2002 16:59:39 +0000

A man was banned from driving for 6 months and fined £300 + £45 costs after

being caught doing 92mph down the A64 in England. "This will now mean commuter belt train travel for my client. The ban will cause all sorts of problems for him at work", said his lawyer. The reason he gave for speeding was that he was late for a business meeting in York, a large city in the North-East, which was caused by a navigation error. After typing "York" into his in-car computer, it dutifully guided him to York, a small village on the opposite side of the country, North-West of Manchester. The man claimed to be "very nervous" when he approached Manchester but trusted the navigation system when it claimed he was "10 miles from York". "When he was driving down the M6 he began to have doubts that it was the right way", said his lawyer, "But he thought 'it must be right, it's a computer'". [Source: *York Evening Press*, 9 Nov 2002]

Or maybe he should read comp.risks more often. Or a map of England :-)

Matthew Bloch Bytemark Computer Consulting Limited +44 (0) 8707 455026

<http://www.bytemark.co.uk/>

[If the man had ever eaten Yorkshire Pudding not knowing where to find a

York shire, he may have been pudding it mildly. Terrier Hair Out!

(The last sentence is a memory test for long-time readers who were reading

RISKS in May 1990.) PGN]

Small things add up

Bill Lamb <blamb@cox-internet.com>

Thu, 07 Nov 2002 23:31:49 -0600

My favorite risks are those little things in life that often seem silly simply because they are - no matter how cool and modern they appear.

I visit a nearby convenience store daily. Over the past few years I have watched as the owners (a small regional chain) converted its cash register to a system that controlled the gas pumps, too. It was a common practice and one that makes sense, I suppose. Later, I watched as a new computerized register system was installed, one with so many buttons, bells and whistles that the store's constantly rotating staff found the system difficult-to-impossible to learn. Still later, a new check system was added. One writes a check, signs it, hands it to the clerk who then runs it through a machine and hands it back to you. I'm sure there is some very logical reason for this apparent silliness. (I mean, why write a check if they're just going to give it back to you? I've watched countless people ask, "What do I do with it now?") The latest change involved adding a credit/debit card unit to the computerized register system. On the whole, you'd think all of this was pretty nifty. But not really.

As I have watched all of this advancement taking place at the store, I have also noticed the lines and waits grow longer and longer. For all the technology they've bought into, the time it takes to service a sale has gone

up tremendously.

Ever try finding and swiping the bar code of a Sunday newspaper on a crowded counter top? It can be a pain, so much so that the clerks now clip and keep one bar code and swipe the little slip of paper over the reader to avoid the hassle.

Credit cards? Wait for clearance, then wait for the ticket to print out, then sign it and get your copy. (Why are those small printers so slow?)

Checks? The same: clearance is slower by far than simply putting the check into the cash drawer like they used to.

It's bad enough when all the systems work, but when one component fails for whatever reason, the poor clerks, who know nothing about the system, are left to try and try again as the rest of us grow impatient in line.

Then today, the ultimate: the entire system died. Nothing worked. At all. People were leaving left and right, but I braved the counter and told the clerk what I wanted.

"Uh ... you have the exact change?" she asked.

Digging in my pocket, I said, "How much is it?"

You guessed it. She didn't know because few of the store's items are priced in English, only via the bar code. And only the computer knew those prices. And it wasn't working.

Another example of humans outsmarting themselves.

[Ah, yes. We had a big storm. Huge power outages, one still going after 24 hours on Friday evening. I just got back from dinner where the restaurant and a large surrounding area lost power; we were the last folks served from gas burners before the kitchen shut down because of no fans. PGN]

✉ Re: 'British' spelling ([RISKS-22.36](#))

"Christopher Allen" <cpcallen@ruah.dyndns.org>
Friday, November 08, 2002 4:39 PM

In comp.risks, Michael (Streaky) Bacon wrote:

> I was raised in Jersey (the Channel Island, not the State). This is part of
> the United Kingdom, but not the European Union (confusing isn't it?)...

I think you may be mistaken, and in any case it's actually a bit worse than that: Guernsey and Jersey **not** part of the United Kingdom but are dependencies of the Crown and so are, as I understand it, consequently considered to be part of Great Britain. This puts them in a situation opposite that of Northern Ireland, which is part of the UK but not Great Britain.

Furthermore, while it's true that the Channel Islands are not part of the EU, my partner - like many Channel Islanders - has an EU

passport
nonetheless, because of English ancestry.

Risks? Assuming that jurisdictions are necessarily
concentric... or that
"The United Kingdom of Great Britain and Northern Ireland"
actually includes
all of Great Britain.

See also: <http://www.fotw.ca/flags/gb-dep.html>

Christopher Allen, Studio 10, 319 Archway Rd. London N6 5AA U.K.
cpcallen-usenet@ruah.dyndns.org <http://ruah.dyndns.org/~cpcallen/>

[PGN adds Michael Bacon's response:

"Mea culpa - I intended to type 'British Isles', it just
came out as

'United Kingdom' - sorry.

It seems that I suffered an even more severe bout of 'finger
trouble',

as I also intended to type 'Gaelic' but it came out as
'Celtic'."]

⚡ Re: What if ... the pundits had nothing ... ([RISKS 22.35](#))

Edward Reid <edwardreid@spamcop.net>

Fri, 8 Nov 2002 15:13:04 -0500

> Modern elections have [...] become opportunities for political
analysts to
> show off by projecting the results before the votes are counted

Of course, much of this prediction is done by projecting from a
few reported
precincts. Pockets of sanity still exist, however. This from the
Gadsden

County Times, Quincy FL, 7 Nov 2002, p1:

Shirley Knight, supervisor of elections [of Gadsden County], took much of the suspense out of the night, when she opted to wait until all of the votes were tabulated to release them, instead of releasing them as the precincts were counted.

"I wanted to keep down any confusion," she said.

⚡ REVIEW: "Information Assurance", Joseph G. Boyce/Dan W. Jennings

Rob Slade <rslade@sprint.ca>
Fri, 8 Nov 2002 08:02:44 -0800

BKIAMOIS.RVW 20021012

"Information Assurance", Joseph G. Boyce/Dan W. Jennings, 2002,
0-7506-7327-3, U\$44.99
%A Joseph G. Boyce
%A Dan W. Jennings
%C 2000 Corporate Blvd. NW, Boca Raton, FL 33431
%D 2002
%G 0-7506-7327-3
%I Butterworth-Heinemann/CRC Press/Digital Press
%O U\$44.99 800-272-7737 <http://www.bh.com/bh/> dp-catalog@bh.com
%P 261 p.
%T "Information Assurance: Managing Organizational IT Security
Risks"

The preface states that this book is distinct because 1) it covers concepts and principles (although how this could be a distinctive is somewhat lost on me: many of the chapters relate directly to six of the ten CBK [Common Body of Knowledge] domains), 2) it promotes a defence in depth strategy (hardly unusual in general security works), 3) it attempts to counter

the perception
of an antagonism between security and operations (fairly
conventional), and
4) it points out resources for added information (and how is
that unique?)

Part one covers the foundational concepts of an organizational IA
(Information Assurance) program. Chapter one defines IA in a
way that makes
it basically the same as any kind of information systems
security, and
offers vague thoughts on the importance of information. There
is a brief
review of some basic security concepts (as well as some that are
not quite
central) in chapter two. Defence in depth is also defined at
this point:
rather idiosyncratically, it is specified to be in opposition to
"security
by obscurity" and perimeter defence.

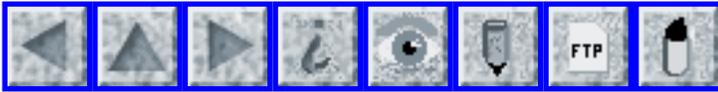
Part two is supposed to look at determining the organization's
current IA
posture. Chapter three purports to help ascertain an IA
baseline, but is
really just a list of possible security technologies.
determining security
priorities, in chapter four, talks about data and resource
classification,
but much of it is vague philosophy, rather than practical
advice. While
summarized in tables rather than text, chapter five's material
on IA posture
is just plain, old risk analysis.

Part three is presumed to help establish a defence in depth
strategy. There
is a basic introduction to policies in chapter six. IA
management, in
chapter seven, is primarily more suited to system
administration. Chapter
eight's look at IA architecture covers subjects and objects, but
has no

security models. The text does review threats and various security technologies, and, very strangely, assumes that the OSI (Open Systems Interconnection) network model can be used as a security structure. Operational security administration, in chapter nine, recycles random concepts that have been presented earlier. Configuration management is held to be software change control, and chapter nine also concentrates on "emergency" changes. Chapter eleven's review of the system development life cycle is terse. Chapter twelve, on contingency planning, is extremely terse, and suggests that you have a backup, UPS (Uninterruptible Power Supply) and a disaster recovery plan. The material on training, in chapter thirteen, is both generic and short. Policy compliance oversight is limited to intrusion detection systems, audit logs, and virus scanning, in chapter fourteen. Chapter fifteen's look at incident response is basic and brief. Finally, chapter sixteen examines IA reporting--and suggests that you have a structure for it.

This work is yet another attempt at a generic security guide. It has no distinctives. In fact, there are simple security guides for home users that do a better job of explaining the structure, process, and technologies.

copyright Robert M. Slade, 2002 BKIAMOIS.RVW 20021012
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

[ACM](#) Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 38

Weds 13 November 2002

Contents

- [Wireless keyboard](#)
[Mike Hogsett](#)
- [Server crash leaves students unable to register](#)
[Max Power](#)
- [Colleges urged not to monitor peer-to-peer sharing](#)
[NewsScan](#)
- [Re: Hartford Public Library Net Browsing - Bugged or Not?](#)
[George Mannes](#)
- [More on the Autotote scam](#)
[PGN](#)
- [Joke not so funny anymore](#)
[Toby Gottfried](#)
- [Chip glitch hands victory to wrong candidate](#)
[PGN](#)
- [Glitches indeed!](#)
[Rebecca Mercuri](#)
- [VoteWatch](#)
[Steven Hertzberg](#)
- [Election integrity in general](#)
[PGN](#)

- [Re: Lynn Landes's analysis of the 2002 Elections](#)
[PGN](#)
[Rebecca Mercuri](#)
 - [Re: Zogby poll failures](#)
[Henry Baker](#)
 - [REVIEW: "Manager's Guide to Contingency Planning for Disasters", Kenneth N. Myers](#)
[Rob Slade](#)
 - [REVIEW: "High Technology Crime Investigator's Handbook", Gerald L. Kovacich/William C. Boni](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Wireless keyboard

Mike Hogsett <hogsett@csl.sri.com>
Mon, 11 Nov 2002 11:31:50 -0800

While a Stavanger man typed away at his desktop computer, his text was also streaming in on his neighbor's machine in a building 150 meters away.

<http://www.aftenposten.no/english/local/article.jhtml?articleID=427668>

All I can say is Why-re-less?

- Mike Hogsett

⚡ Server crash leaves students unable to register

Max Power <mikehack@u.washington.edu>
Tue, 12 Nov 2002 18:23:46 -0800 (PST)

The five servers that handle Washington University's class registration crashed on 8 Nov 2002, preventing several thousand students from signing up for their winter-quarter classes for most of the day. This was attributed to a system software problem rather than an overload problem: The software translating students' Net IDs into student numbers was running much slower than previously. 14,000 students were eligible to register, as opposed to only 1,000 in the spring quarter. Ironically, this came shortly after the Registrar's Office had permanently shut down its Student Telephone Assisted Registration system (STAR), because of phone-line costs and lack of use.

[Source: Alex Sundby, *The Daily*, Washington University, 12 Nov 2002; PGN-ed]

<http://www.thedaily.washington.edu/all.lasso>

[?&-database=DailyWeb.fp5&-layout=List&-response=newspage.lasso&-recordID=33782&-search&-Token.Count=3](http://www.thedaily.washington.edu/all.lasso?&-database=DailyWeb.fp5&-layout=List&-response=newspage.lasso&-recordID=33782&-search&-Token.Count=3)

⚡ Colleges urged not to monitor peer-to-peer sharing

"NewsScan" <newsscan@newsscan.com>

Mon, 11 Nov 2002 10:05:51 -0700

The Electronic Privacy Information Center (EPIC), a Washington-based nonprofit organization that promotes freedom of speech on the Internet, is attacking letters recently written by the recording industry asking college officials to monitor Web use at their institutions for copyright violations made through peer-to-peer sharing of music or video files by

members of the academic community. EPIC is criticizing those letters for trying to shift the burden of content enforcement to academic institutions which have scarce resources for such purposes, and is warning against a network "arms race" between file sharers and copyright enforcers. The group thinks colleges should avoid adopting a "confrontational role with respect to these technologies," because all it would do would be to harm the network's overall performance. [IDG News Service 11 Nov 2002; NewsScan Daily, 11 Nov 2002]

<http://www.idg.com.hk/cw/readstory.asp?aid=20021111002>

✦ Re: Hartford Public Library Net Browsing - Bugged or Not? ([R-22.35](#))

<George.Mannes@thestreet.com>

Mon, 11 Nov 2002 11:54:39 -0500

Bill Olds' *Hartford Courant* column "The FBI Has Bugged Our Public Libraries" was excerpted starkly in [RISKS-22.35](#). The column apparently cited "anonymous sources". The FBI responded, claiming the information was false, and the paper now admits it should have been more rigorous in checking the details. Olds said, "I called the Justice Department but I was told they could not discuss issues involving the FBI and libraries. ... In the atmosphere of secrecy created by the Patriot Act, my sources misinterpreted what the FBI was doing." As Don Sellar,

ombudsman at *The Toronto Star*, once said, "When the sources are wrong, they're wrong anonymously and it's the newspaper's credibility that gets publicly dented."

[Source: "Anonymous Sources, Bad Information", Karen Hunter, *Hartford

Courant*, 10 Nov 2002; PGN-ed]

<http://www.ctnow.com/news/opinion/columnists/hc-hunter1110.artnov10,0,6354989.column>

George Mannes, 14 Wall Street - 15th Floor / New York, NY 10005
phone: 212-321-5208 / mobile: 917-207-5790 george.
mannes@thestreet.com

✦ More on the Autotote scam ([RISKS-22.35](#))

"Peter G. Neumann" <neumann@csl.sri.com>

Wed, 13 Nov 2002 10:20:18 PST

The saga of the PickSix winner that culminated in a wild-card bet on every horse in the Breeders' Cup Classic (the horse race with the U.S.'s largest pot) continues, and provides a timely set of lessons, for example:

- * The intense risks of insider misuse in certain types of systems
 - * The perils of poor system designs that seriously ignore security
 - * The importance of audit trails, and especially nontamperable ones
 - * The value of truly independent unbiased objective security audits
- by really knowledgeable and experienced red-teaming experts

Whenever such an unusual event involving a large payout is

detected, an immediate concern should be this: Have there been other similar cases that were not previously noticed? In the Breeders' Cup case, it was soon thereafter discovered that the same type of scam had been pulled at least twice previously, and that all of the apparent participants are linked by a bond of fraternity brotherhood from their undergraduate days at Drexel University. In each subsequently uncovered scam, as well as in the Breeders' Cup case, an off-track bet from a particular betting parlor that did not keep records of phone-in bets was subsequently altered by insider system manipulation AFTER the results of the early races were known, but before the records were transmitted to the central facility. [If you want the background on the cases and the individuals involved, see the series of articles in *The New York Times*, 9 Nov, 10 Nov, and 13 Nov.]

And then, you might ask, have there been other cases of undetected insider fraud in gambling systems? There have certainly been publicly admitted precedents of rigged gambling payoffs, perhaps most notably the Harrah's Tahoe \$1.7 million progressive multiple-slot-machine jackpot that reportedly was triggered by insiders, although the exact details of that event almost 20 years ago are still not widely known. We have also noted in RISKS that you might want to wonder about the trustworthiness and integrity of on-line gambling systems. But perhaps MOST INSIDIOUS from the effect on the populace at large is that implicit in all those discussions are that the

same concerns arise in the all-electronic voting machines, as noted in recent RISKS issues (including this one). In the horse-race betting cases, even if there had been audit records as to the exact bets that were later altered (there were no such audit trails on the OTB system used for the exploits), a really clever perpetrator with insider access privileges might have been able to alter the audit records without being detected unless the audit mechanism was totally nontamperable (which is generally considered to be either overkill or practically impossible despite the existence of once-writable media). In all computing environments where something is valued (especially gambling, electronic voting, national security, intelligence, counter-intelligence, supposedly secure databases with stringent privacy policies, etc.), the presence of overprivileged insiders and the absence of nontamperable audit trails must both be considered as warning indicators.

⚡ Joke not so funny anymore

"Toby Gottfried" <toby@gottfriedville.net>
Mon, 11 Nov 2002 08:46:31 -0800

I am reminded of an old election joke, which seems like less and less of a joke.

A third world country decided to go democratic, turning to the USA for guidance. On a limited budget, they could only afford second-

hand

equipment and got some voting machines from the city of Chicago.

With great fanfare, they held their election, with Fyodor Guantanamo running against Kwame Santahara.

The winner was ...

Richard J. Daley.

⚡ Chip glitch hands victory to wrong candidate

"Peter G. Neumann" <neumann@csl.sri.com>

Tue, 12 Nov 2002 13:43:00 PST

In Nebraska, a defective computer chip in Scurry County's optical scanner misread ballots Tuesday night and incorrectly tallied a landslide for the wrong party. Investigation led to the diagnosis of a faulty chip, which when replaced reversed the outcomes in two commissioner races, verified by a hand recount, from Republican victories to Democratic victories.

[Source: http://www.truthout.org/docs_02/11.13C.vote.chip.htm; PGN-ed]

For some other irregularities in Nebraska, see VoteWatch (next item).

⚡ Glitches indeed

"Rebecca Mercuri" <notable@mindspring.com>

Tue, 12 Nov 2002 19:20:49 -0500

You think the November 5, 2002 US General Election went smoothly?

Use your favorite Web engine and search for the words "election" and

"glitch" -- a recent scan on Google News turned up hundreds of press

reports. Not all of these troubles were in Florida -- states included Texas,

Alabama, Nevada, Georgia, California, South Carolina, Nebraska, and New

Jersey. Voter News Service, the agency that provides exit poll data that

might have been used as a cross-check against computerized returns, was

coincidentally knocked out of service by an unidentified "massive computer

glitch" on election day as well. Many of the election problems (including

those at VNS) occurred in spite of hundreds of millions of dollars (soon to

be billions) spent on new equipment. If, say, an automobile manufacturer

experienced numerous major "glitches" in a product line, the public would be

clamoring for a recall. Yet everyone seems quite content with these

computerized voting systems, and the press continues to blame the poll

workers, even in Broward County where they spent an additional \$2.5M on

training and staff for election day and still managed to misplace some

103,000 votes. Characterizing these serious problems as "glitches" makes it

seem like poor engineering and incompetent election system management is

somehow acceptable to the American public. It's not. A massive recall of

these inappropriate and defective devices must be started immediately. Call

or write to your Secretary of State and complain.

Rebecca Mercuri www.notablessoftware.com/evote.html

VoteWatch

"Steven Hertzberg" <stevenhertzberg@hotmail.com>

Mon, 11 Nov 2002 23:32:23 -0800

I recently launched VoteWatch.us, which is an online service that allows voters to immediately report voter machine errors, polling place problems and other voting obstacles. VoteWatch is quickly becoming the central repository of election 2002 discrepancies.

I would appreciate it if you could browse VoteWatch and add comments as you see fit.

Steven Hertzberg, Founder, VoteWatch, San Francisco, CA

Election integrity in general

"Peter G. Neumann" <neumann@csl.sri.com>

Mon, 11 Nov 2002 11:44:40 PST

With PAPER BALLOTS, there is the accountability of the paper ballots themselves, which can potentially be examined for serial number consistency, watermarks to hinder the introduction of phony ballots, fingerprints, etc.

With LEVER MACHINES, it is true that they can be rigged to fail to record votes for one candidate, but it is unlikely that such a vote could be misrecorded for another candidate (assuming the standard ballot face is in place).

With PUNCH-CARDS and MARK-SENSE CARDS, there is the evidence of the cards themselves. Although tampering with the cards is obviously possible (substitution, invalidation by internal fraudulent overvoting by election officials, the cards provide an audit trail).

With the ALL-ELECTRONIC SYSTEMS that exist today (with the exception of the Avante system that now includes the Mercuri Mechanism as a standard), there is ABSOLUTELY NO EVIDENCE OF ANYTHING OTHER THAN THE ALLEGED BALLOT IMAGE -- which itself can be fraudulent, given proprietary code, Trojan horses and trapdoors, etc. Recounts are meaningless if the data is already corrupted when stored. Furthermore, many of these machines are configured by vendor-supplied personnel, with potential access privileges for the system or the accuracy of the configuration.

Every one of these systems has potential problems. But a world-wide consensus seems to suggest that a single piece of paper with a single set of candidates is the most reliable method, because poll watchers can see what is happening. How do you watch the bits moving around inside an all-electronic system?

✉ **Re: Lynn Landes's analysis of the 2002 Elections ([RISKS-22.37](#))**

"Peter G. Neumann" <neumann@csl.sri.com>

Mon, 11 Nov 2002 7:33:43 PST

I received several responses strongly offended by the inclusion of Lynn Landes's piece in [RISKS-22.37](#). I deeply regret if that item offended you. I included it not primarily for its claims (whether accurate or not), but rather for the implications of accidents and misuses, potential and actual, publicized or kept secret, detected and undetected, that we have been discussing in RISKS for many years. Much of her piece is actually relevant here, although I think her message may have been weakened because of certain statements that were more political than the objective reporting that we try to make the expected norm in RISKS.

As I see it, the most important question we should be asking is this:

With respect to those of you who voted last week using an all-electronic voting machine, is there any meaningful assurance that the vote you cast was correctly recorded -- that is, any assurance that there were no misconfigured systems, accidents, internal fraud, etc.? For almost all of the existing electronic systems (with the exception of one that actually incorporates the Mercuri Mechanism -- namely, Avante), the answer is an UNEQUIVOCAL NO. This is an untenable situation if you believe

in election
integrity, IRRESPECTIVE of your party affiliations. PGN

✦ **Re: Lynn Landes' analysis of the 2002 Elections ([RISKS-22.37](#))**

"Rebecca Mercuri" <notable@mindspring.com>

Mon, 11 Nov 2002 00:02:11 -0500

First of all, it's more like \$4B, Lynn wasn't including the additional sums for training and so on that were also authorized by the Help America Vote Act bills. But even \$4B is just the tip of the iceberg.

Over in Broward County Florida, where they just spent around \$18M for brand new touch-screen voting machines they found that they had to pay an additional \$2.5M just to run the November election, because the machines couldn't be set up and monitored by the regular poll workers who are normally hired. Now if Broward has to pay this sum 2 times a year for the next decade, how does this Help America Vote? They could print up an easy-to-read paper ballot for every man, woman, and child in the entire County for well under \$1M and they would probably not discover missing cartridges 2 days later with 103,000 missing votes on them (after being monitored by the Republicans who came down from the state to help the Democrats out with the election). A box of paper ballots is a lot harder to lose (not that it hasn't been done) than a small voting cartridge. And the

paper ballots can be read by hand if the computers are misprogrammed (like they seem to have been in a lot of US counties this past November).

Over in Texas, I don't really see how it's could be the Democrats' fault when they discovered their brand new touchscreen voting machines lighting up for the Republican candidates over in Dallas last week. When the Democrats sued to stop the machines being used, the Republicans said "we haven't had any complaints." Sure, because they didn't light up for Democratic candidates when the Republicans were pressed. I wonder why? Misalignment? Conveniently, none were misaligned in the other direction. Hmmm.

If you really look at your history books, you'll see all sorts of election fraud in all sorts of places. We had things like literacy tests. And we had to pass amendments to the US Constitution so that gender and race wouldn't be used to prevent citizens from voting. There's plenty of election fraud too. Tip O'Neil (the late Speaker of the House) described in his autobiography (after he retired) a scheme whereby paper ballots were routinely substituted (called chain voting). It's not any particular party that is to blame, it's just that vote stealing is as much a tradition in the USofA as apple pie. Unauditable voting machines just make it even easier to cover up.

Folks can continue to stick their heads in the sand and pretend this hasn't happened, doesn't happen, and won't happen. Or they can face reality and

then work to adopt systems that will REDUCE and ELIMINATE election fraud, rather than encourage and enhance the ease of doing it.

Please read the additional material and links on my website over at www.notablessoftware.com/evote.html and join the effort to save democracy before it's too late.

R. Mercuri

✶ Re: Zogby poll failures (Landes, [RISKS-22.37](#))

Henry Baker <hbaker1@pipeline.com>

Sat, 09 Nov 2002 14:56:54 -0800

There was a long article in the *Wall Street Journal* with lots of quotes from Zogby. Apparently, the problem is that they depend upon telephone solicitation to find out how people are voting, and people are using caller ID to screen out the calls. There is also a significant rise in the percentage of cell phones, for which spam telephone calls aren't allowed. Also, women are not as at home as they used to be, so there's no one to answer the phones.

So there's no need to attribute malice to the bad polling data, when simple incompetence will do just fine.

[... and an inherently flawed methodology? PGN]

🔥 **REVIEW: "Manager's Guide to Contingency Planning for Disasters",**

Rob Slade <rslade@sprint.ca>

Tue, 12 Nov 2002 08:01:03 -0800

Kenneth N. Myers

BKMGTCPD.RVW 20021012

"Manager's Guide to Contingency Planning for Disasters", Kenneth N. Myers,

1999, 0-471-35838-X, U\$55.00

%A Kenneth N. Myers

%C 5353 Dundas Street West, 4th Floor, Etobicoke, ON M9B 6H8

%D 1999

%G 0-471-35838-X

%I John Wiley & Sons, Inc.

%O U\$55.00 416-236-4433 fax: 416-236-4448

%P 234 p.

%T "Manager's Guide to Contingency Planning for Disasters"

The preface clearly states that this book promotes a "what if," worst case

scenario approach to contingency planning. It presents the development of

detailed business continuity procedures as a waste of time, and assumes that

minor mishaps can be handled within the limits of the methods meant to deal

with the worst case. Although this flies in the face of conventional BCP

(Business Continuity Planning) wisdom, in all but the last item Myers makes

a convincing case. The emphasis is on avoiding the "how long can you do

without" type questions so common in BCP, and more directed towards "what

alternatives can we use when we have to do without" answers.

Chapter one is an introduction, and this is obviously not your average DRP (Disaster Recovery Planning)/BCP book, since it includes items such as a "disaster life cycle." "Defining The Problem" doesn't really happen in chapter two, although one could say that the problem is clarified to a certain extent. The text is a bit repetitive, reiterating several times that too many companies concentrate on recovering the technology before the business. There is more traditional look at BCP in chapter three, since it concentrates on awareness and education, and provides a good, basic overview of selling the contingency planning idea to management. Chapter four reviews project planning, although primarily from an outsider perspective, like that of a consultant. From this viewpoint, it offers very practical, helpful advice. Business impact analysis is presented in chapter five, although, again, the text retails content already stated elsewhere. The implementation strategy, in chapter six, primarily covers dealing with various layers of management. The Myers process of plan development is presented in a structured form in chapter seven, although most points have been made already. Chapter eight again presents a more traditional, and very short, view, this time of plan maintenance, education, and testing. The guidelines for internal consultants and consulting firms, in chapter nine, form a nice checklist.

There are a number of appendices, of which B (with a sample contingency plan and examples of alternative methods is particularly useful. A

broader list
of alternative methods is suggested in Appendix C.

While some may dismiss it as a kind of cost/benefit reductio ad
absurdum,

Myers' method does raise issues that need to be considered.

This contrarian

view should be more widely considered by the BCP community.

copyright Robert M. Slade, 2002 BKMGTCPD.RVW 20021012
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

★ **REVIEW: "High Technology Crime Investigator's Handbook",**

Rob Slade <rslade@sprint.ca>

Wed, 13 Nov 2002 08:05:55 -0800

Gerald L. Kovacich/William C. Boni

BKHTCRIH.RVW 20021012

"High Technology Crime Investigator's Handbook", Gerald L.
Kovacich/William C. Boni, 2000, 0-75067806-X, U\$34.95

%A Gerald L. Kovacich shockwavewriters.com

%A William C. Boni

%C 2000 Corporate Blvd. NW, Boca Raton, FL 33431

%D 2000

%G 0-75067806-X

%I Butterworth-Heinemann/CRC Press/Digital Press

%O U\$34.95 800-272-7737 <http://www.bh.com/bh/> dp-catalog@bh.com

%P 298 p.

%T "High Technology Crime Investigator's Handbook: Working in
the

Global Information Environment"

The preface makes the somewhat contradictory statement that the
book

is "not a 'how to investigate high-technology crime' book but

provides

basic information for someone ... new to the profession." This odd assertion may be partially explained by the fact the text is very heavy on career and organizational matters, and extremely light on functions and technology. It would appear that any technical issues are seen as "how to," while corporate politics are basic information.

Part one provides an introduction to the high technology crime environment, in broad overview. Chapter one is a pedestrian presentation of high technology. The text is very disjointed (a discussion of government departments using high-tech crime as a justification to fight for increased budgets is immediately followed by a minor example of online harassment), and, despite the promotion of the importance of technical information and tools for crime investigation, the technical material is weak, simplistic, and oddly handled. For example, a subjective and imprecise measure of data volume (a book) is used to calculate ridiculously "accurate" (in terms of significant figures) store sizes for a variety of obsolete systems. There is a superficial and pessimistic look, in chapter two, at the "Global Information Infrastructure." Again, the technical content is insubstantial: mention of lists of top level domains makes reference to using a search engine to find them, but the instructions consist of "well, you're an investigator, investigate." This seems to sum up the attitude to providing necessary information. High-technology miscreants, in chapter three, are reasonably well described, with only minor errors. There is an internal contradiction when the text lumps phone phreaks in with hackers, and then treats them as distinct,

and
the book retails the Cap'n Crunch myth, whereas Draper himself
points
out that he was taught about the 2600 hertz whistle. There is a
slight overemphasis on the importance of "professional hackers."
Chapter four's coverage of attack technology is jumpy and
fragmented.
An "ISP attack" makes little sense, while spoofing is narrowly
defined
to include only one specific type of session hijacking. Three
pages
of diagrams of PBX (Private Branch eXchange) attacks explain
nothing.
Protection technology, in chapter five, is defined as access
control,
accountability, and audit trails, followed by a random grab bag
of
security ideas.

Part two is an overview of the high technology crime
investigation
profession or unit. This material is basically recycled from
"The
Information Systems Security Officer's Guide," by one Gerald L.
Kovacich. There are a large number of very short chapters.
Chapter
six is a generic promotion for career planning, with added, but
oddly
irrelevant, details. Marketing yourself, in terms of
preparation of
resumes and for interviews, is in chapter seven. Chapter eight
describes the perfect, and therefore fictional, company to work
for.
This is followed by the perfect job description in nine, the
perfect
investigative unit in ten (with some brief staff job
descriptions in
eleven), and the perfect mandate (plus an excessively detailed
example
of a PBX survey) in chapter twelve. Chapter thirteen suggests
that
you develop contacts, but, somewhat in opposition to the career
building emphasis earlier, this concentrates on "sources" or

informers. The development of metrics, in chapter fourteen, seems to be primarily concerned with the creation of bar charts to show management that you've been working. The "Final Thoughts," in chapter fifteen, are mostly vague opinions.

Part three is entitled high technology crimes and investigations. Chapter sixteen has various stories, with almost no detail, about crimes and computers, few of which are relevant to corporate investigations. There is some useful advice, in chapter seventeen, on the initial seizure and chain of custody of computer equipment, but the discussion is limited to data recovery.

Part four is supposed to be about challenges to high technology crime investigation, but chapter eighteen, the only section, simply contains more vague thoughts.

For someone trying to build a career via political maneuvering, this book can provide some useful tips. For someone trying to investigate a crime involving computers, it might be a bit frustrating.

copyright Robert M. Slade, 2002 BKHTCRIH.RVW 20021012
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

<http://victoria.tc.ca/techrev> or <http://sun.soci.niu.edu/~rslade>



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

[ACM](#) Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 39

Saturday 23 November 2002

Contents

- [More on the Breeders Cup Pick-6 fix](#)
[Danny Lawrence](#)
- [Crackers steal 52,000 university passwords](#)
[Monty Solomon](#)
- [Slashdot suggests X-Box gamezone open to DoS](#)
[George Michaelson](#)
- [Laptop injures lap](#)
[Gene Spafford](#)
- ["AccuVote" comes to Boston -- argh!](#)
[Jonathan Kamens](#)
- [NSF FastLane promotes excessive sharing?](#)
[Lee Rudolph](#)
- [Interesting new spammer trick](#)
[Jonathan Kamens](#)
- [Bad assumption in automated toll collection](#)
[Andrew Goodman-Jones](#)
- [REVIEW: "Security Engineering", Ross Anderson](#)
[Rob Slade](#)
- [REVIEW: "Network Intrusion Detection", Northcutt/Novak/McLachlan](#)
[Rob Slade](#)

 [Info on RISKS \(comp.risks\)](#)

More on the Breeders Cup Pick-6 fix

Danny Lawrence <Danny@TiassaTech.com>

Thu, 21 Nov 2002 13:07:40 -0500

Unsurprisingly, the *Daily Racing Form* is doing a better job of covering the scam than the general media, here are a couple of references:

The "3rd member" of the party (whose account was used to make the "test runs" of the fix prior to the Breeders Cup) was already under investigation by the OTB

http://www.drf.com/members/web_news.generate_article_html?p_news_head=42153&p_arc=1

The fired Autotote employee pleads guilty to one count of wire fraud:

<http://www.drf.com/news/article/42458.html>

Also it seems that he (and his 2 confederates) were cashing unclaimed tickets that he found in the Autotote system.

As in many cases of this type it looks like greed was their undoing.

Here's a link to another betting scam from the 1970's:

http://www.drf.com/members/web_news.generate_article_html?p_news_head=42077&p_arc=1

I think that the fact that the OTB was already looking into the 3rd person's suspect account indicates that the checks were there, that they didn't act sooner indicates prudence on their part. The worst thing (from a creditability standpoint) that a betting organization can do is withhold a payout and accuse a player of cheating, only to be proved wrong.

--Danny Lawrence, Tiassa Technologies Inc.

<http://www.tiassatech.com/domino/saga.nsf/story/uk>

✶ Crackers steal 52,000 university passwords

Monty Solomon <monty@roscom.com>

Wed, 20 Nov 2002 02:05:07 -0500

The University of Oslo had to change the passwords of 52,000 users and reinstall software on dozens of computers after crackers managed to infiltrate the network and extract the institution's central password file.

<http://www.aftenposten.no/english/local/article.jhtml?articleID=437439>

✶ Slashdot suggests X-Box gamezone open to DoS

George Michaelson <ggm@apnic.net>

Fri, 22 Nov 2002 10:59:30 +1000 (EST)

UNPROVEN RISK

gamers with modded XBoxes are banned by Microsoft. banning means they can be recognized. recognition requires a unique ID, the pozited unique ID is serial no and MAC address.

Xbox hackers allege that by changing serial number and MAC address and turning off their modchip they succeeded in registering in Xbox gamezone.

Therefore, since integers between 0 and the size of the register in the chip are a finite resource, they have 'stolen' some unsold/unregistered machines ID.

Therefore there is an identity theft risk.

And there is a DoS game here: walk the space, with your modded box, and lock out the entire XBox userspace from the gamezone

Yes, its a large numberfield, maybe a 128-bit sequence space. But I bet you can walk it for fun and profit...

>From SlashDot:

>Changing serial numbers and macs...

>by AtariDatacenter on 11:11 AM November 22nd, 2002 (Score:5, Insightful)

>(#4727735)

>(User #31657 Info) <mailto:jmccorm@yahoo.com>?

Subject=SlashdotResponse Neutral

>

>

> So they said they changed their serial number *and* MAC address to

> get back on. This is interesting and points back to something someone said in a previous thread. All you need to do is to make

> a program to burn through serial number space and get them marked

> invalid, and you've got a DoS of entertaining proportions.

Laptop injures lap

Gene Spafford <spaf@cerias.purdue.edu>

Fri, 22 Nov 2002 18:23:57 -0500

There are all kinds of new risks with higher-power processors and metal cases:

<http://www.cnn.com/2002/WORLD/europe/11/22/health.laptop.reut/index.html>

[Alo noted by Mark Brader. PGN]

⚡ "AccuVote" comes to Boston -- argh!

Jonathan Kamens <jik@kamens.brookline.ma.us>

Thu, 14 Nov 2002 22:06:38 -0500

[A letter I'm about to send to the Massachusetts Secretary of State and the City of Boston's Election Department:]

Dear Sirs,

I was dismayed to learn recently that the City of Boston has decided to replace its lever-activated voting booths with Diebold AccuVote-OS machines, and indeed has already purchased the Diebold machines.

As you may know, with the Diebold machines you mark your votes by coloring in circles on a paper ballot, then you feed the ballot through the machine and into a ballot box. After you feed your vote through the machine, a count of successful votes displayed by an LED on the front of the machine is incremented.

I asked the volunteer demonstrating the machine to me, "But how do I

know that the machine recorded my vote correctly?" In response, she told me that since the number was incremented, my vote was counted. I didn't even try to make her understand that since a ballot could have multiple races on it, and since I could abstain from any of them by not filling in any of the circles for that race, there was no way for me to distinguish between the machine correctly registering all the votes I recorded and the machine registering some of them and missing some and treating them as abstentions. Not to mention the possibility that the machine might register my votes wrong, rather than just register some abstentions where I actually voted.

It's certainly a good thing that this voting machine uses a paper ballot. Such a human-readable, physical record of each vote is an essential part of any reliable voting system, electronic or otherwise.

However, without explicit acknowledgment from the machine to the voter of which votes were and were not registered, and a chance for the voter to correct any errors or omissions revealed by that acknowledgment, the functionality provided by this machine is simply not adequate for reliable, accurate voting.

Furthermore, I cannot help but wonder what happens if the machine says that it didn't successfully register my vote, if the back of the machine feeds directly into a ballot box as the volunteers at my polling place led me to believe it would. Presumably the ballot box is locked, so they can't remove my first ballot. Do I get to try again? And what if there is then a recount of the paper ballots, and my first ballot is legible the during the recount -- I got to

vote
twice!

In short, this technology is simply not acceptable. I am deeply disturbed that the City of Boston has chosen to ignore the reams of scholarly evidence of this fact and went ahead with the purchase of simply inadequate voting technology.

If you are unfamiliar with all the evidence of why most electronic voting machines are inadequate and of how electronic voting might be done properly, a good place to start researching it is at the Web site of Rebecca Mercuri, "<http://www.notablessoftware.com/evote.html>".

Thank you for your time.

Sincerely, Jonathan Kamens

⚡ NSF FastLane promotes excessive sharing?

Lee Rudolph <lrudolph@panix.com>
12 Nov 2002 14:00:54 -0500

I'm in the middle of preparing a grant proposal for the National Science Foundation, using FastLane, NSF's (now mandatory) online system for proposal preparation, submission, reviewing, etc. For the first time in my grant-writing life, I'm going to have "Co-PIs" (co-Principal Investigators; I am the PI on this proposal). Each Co-PI has to be able to log in to access and modify the proposal; (Co)-PIs' names must be entered

on the
"Cover Sheet" form, and that form states that "Only Co-PIs
entered here will
be available on other forms in this proposal."

How must they be entered? "To add Co-PIs, enter the SSNs of the
Co-PIs and
then save the remainder of the cover sheet by clicking on the
"OK" button at
the bottom of this screen."

In other words (as I have confirmed with a phonecall to the
FastLane help
desk), *either* my Co-PIs have to give me their Social Security
numbers so
that I can enter them on this form (and thereafter they can log
in by
themselves), *or* I have to give my Co-PIs my FastLane password
(and my SSN,
that being [unfortunately] required as well as the password to
log in) so
that they can log in as me and enter their own SSNs (and
thereafter log in
by, but not necessarily *as*, themselves).

Of course, there's a third choice, the one I will actually make:
I can walk
over to each Co-PI's office in turn, log in to FastLane on that
Co-PI's
computer, and let him or her enter his or her SSN. That's easy
enough;
we're all working at the same university. However, if we were
at several
universities several hundred miles apart, using FastLane to
*facilitate
collaboration* among distant colleagues (one of its purported
reasons for
being), this third choice would not be quite so practical.

The RISK is left to the reader.

Interesting new spammer trick

Jonathan Kamens <jik@kamens.brookline.ma.us>

Thu, 14 Nov 2002 09:56:17 -0500

Since many of you are interested in the topic of E-mail spam, e.g., the techniques used by the spammers to evade filtering and the techniques used by everybody else to try to outsmart them, I thought you might be interested in the following new spammer trick which I first saw on October 17 and have seen numerous times since then.

I use a home-grown script to analyze the "Received:" headers of the spam that I receive, determine the appropriate sites to whom to complain, and generate the complaint messages. Spammers figured out quite a while ago to insert forged Received: headers in their messages, but they're usually pretty easy to weed out, e.g., they refer to nonexistent hosts, they list bogus envelope recipients, they have bogus dates, the destination host of one Received: header doesn't match the sender host of the next one in the chain, etc. However, at least one spammer has figured out how to forge a Received: header which more convincing than any I've seen. Here are some of the headers of a spam message I received on October 17:

```
Received: from pacific-carrier-annex.mit.edu (PACIFIC-CARRIER-ANNEX.MIT.EDU [18.7.21.83])
```

```
    by jik.kamens.brookline.ma.us (8.12.5/8.12.5) with  
ESMTP id g9HBd2aP009915
```

```
    for <jik@kamens.brookline.ma.us>; Thu, 17 Oct 2002  
07:39:02 -0400
```

```
Received: from 146-153-179-208.pajo.com (146-153-179-208.pajo.  
com [208.179.153.146] (may be forged))
```

by pacific-carrier-annex.mit.edu (8.9.2/8.9.2) with
SMTP id HAA12722

for <jik@mit.edu>; Thu, 17 Oct 2002 07:39:01 -0400
(EDT)

Received: from 13217 (20458 [53.86.86.54])
by 6432 (8.12.1/8.12.1) with ESMTMP id 27244
for <jik@mit.edu>; Thu, 17 Oct 2002 04:39:00 -0700

From: "Consult" <wizard_21@360.ru>

To: "jik@mit.edu" <jik@mit.edu>

Subject: Êîïïüþðåðû è êîïïëåêðòþùèå îî ÑÀÏÛÏ îèçêèî öåíàî.

Date: Thu, 17 Oct 2002 04:39:00 -0700

Message-ID: <811325562@mlnCplw1hgx>

Note the last Received header. Both the date and the envelope recipient listed in it are correct, and the rest of the header is pretty much formatted correctly; the only tip-off that something strange is going on is the numeric host names. But whoever is doing

this got a little smarter pretty quickly. Here's the last Received:

header from a spam message I receive on November 6:

Received: from delphi.com (mailexcite.com [85.34.182.181])
by aol.com (8.11.6/8.11.6) with ESMTMP id 9874
for <jik@mit.edu>; Wed, 6 Nov 2002 09:37:38 +0000

Much better, eh? I've seen various incarnations of this since then with data that seems at first glance to be correct but does not withstand closer inspection.

Note that you can't use a simple regular expression match to filter out all messages with headers in this format, because this is a valid Received: header format and I've received real non-spam messages that use it (albeit with data that isn't bogus).

They're getting smarter. I just hope by bogofilter database can keep up with them :-).

✶ Bad assumption in automated toll collection

"Andrew Goodman-Jones" <goodie@ozemail.com.au>

Thu, 14 Nov 2002 17:09:47 +1100

eTags are (optionally) used in Sydney for automated highway toll collection.

[risk #1 - well known - loss of privacy]

Background:

If the tag does not read electronically, then your licence plate is photographed. Before sending out an infringement notice, they lookup your licence plate on the database of eTag account holders. In Sydney we have many different types and colours of licence plates (for fashion reasons) and the type of plate forms part of the unique key. [risk #2 - makes identity harder] Motorcyclists are not allowed to have eTags because they haven't found a secure way to attach them to motorcycles.

My friend Robyn had this experience:

I have an eTag for my car which I have used on my bike on a number of occasions. Once it didn't work when I used it on my bike so I thought rather than wait to get a fine I'd ring them. Although they did tell me I should not be using it on my bike they said it didn't matter because it had come up as a misread on my account and that they had just automatically charge my account anyway.

The interesting thing is that I had not told them that I have a bike!!!

So how did they know to charge it to my account ???

Well, the number plate [licence plate] on my car is exactly the same as the number plate on my bike (car has black & white plate with 2 letters & 3 numbers the same as the bike plate but its yellow).

So basically if you have a number plate on your bike that is the same as a car with an eTag you can go through the express lane and it will just get charged to someone else's account. (A bit of a worry if you're the account holder.)

Robyn

[The main risk, #3, their licence plate database apparently does not seem to include the colour of the plate in the field.]

[Robbin' Robyn to Pay Pal? That's Round-Robyn. PGN]

REVIEW: "Security Engineering", Ross Anderson

Rob Slade <rslade@sprint.ca>

Mon, 18 Nov 2002 08:14:55 -0800

BKSECENG.RVW 20021015

"Security Engineering", Ross Anderson, 2001, 0-471-38922-6, U \$65.00

%A Ross Anderson ross.anderson@ieee.org rja14@cam.ac.uk

%C 5353 Dundas Street West, 4th Floor, Etobicoke, ON M9B 6H8

%D 2001

%G 0-471-38922-6
%I John Wiley & Sons, Inc.
%O U\$65.00 416-236-4433 fax: 416-236-4448
%P 612 p.
%T "Security Engineering: A Guide to Building Dependable
Distributed
Systems"

The preface states that this book is intended as a text for self-study or for a one term course, a reference for professionals, an introduction to the underlying concepts, and an original scientific contribution in terms of the foundational principles for security engineering. A very tall order to promise, but one which, for once, seems to have been fulfilled. I have often been asked, in regard to these reviews, whether there are, in fact, any books that I like. Well, I like this one. If you are involved with security and you haven't read it, you should.

Part one deals with the basic concepts of engineering and security. Chapter one presents four example situations of security needs. Protocols are not limited to the precise but limited structures computer people are familiar with. A set of more conceptual, but more formal, authentication problems and protocols are advanced in chapter two. It is unlikely that the models presented exhaust the field, but some thought indicates that they are applicable to a wide variety of applications. (Anderson's writing is clear enough, but he does betray a taste for symbolic logic that might limit the audience for the book. Still, perseverance on the part of the reader will be amply rewarded.) Much the usual thoughts and advice on

passwords is issued in chapter three, although the research is better documented, and some additional research (passphrase generated passwords are as secure as randomly assigned ones, and as memorable as naively chosen ones) is presented. It is strange not to see any mention of the work factor of passwords overall. Chapter four reviews access control, but primarily from the perspective of system and hardware internals. Cryptography, in chapter five, is covered reliably and well, although Anderson does not work overly hard to make the material easy to follow. The problems of distributed systems are examined; in terms of concurrency, failure resistance, and naming; in chapter six.

Part two uses a number of applications of secure systems to introduce particular concepts or technologies. Chapter seven discusses multi-level security, which encompasses most of the formal security models such as Bell-LaPadula. Medical (and census) databases are used, in chapter eight, as examples of multilateral, or compartmented, security: the need to deal with information of equal sensitivity, but restricted to different groups. There is good discussion of inference and aggregation problems. Integrity controls, particularly related to the banking system and fraud, are presented in chapter nine, although the material is long on anecdotes, and contains weaker analysis than the preceding text. Chapter ten reviews monitoring systems, of both monitoring and metering types. In regard to

nuclear command and control systems, chapter eleven examines the tension between availability (the ability to fire a missile) and confidentiality (or authentication: making sure nobody else does). Various aspects of the technology for security printing and seals is dealt with in chapter twelve. Biometrics, in chapter thirteen, gets a good, but fairly standard, treatment. Chapter fourteen delves into tamper-resistance in cryptographic gear and smartcards. The TEMPEST and Teapot (no, I'm not kidding) projects on emission security are reviewed in chapter fifteen. There is good coverage of the basics of traditional electronic warfare in chapter sixteen, although the material on information warfare is not as thorough. Chapter seventeen looks at telecommunications system security, with some material on phone phreaking and lots on cellular encryption. Network attack and defense, in chapter eighteen, is less focussed than other chapters, and adds malware. (There is an odd, and unexplained, assertion that malware would formerly have merited a full chapter: In correspondence, Anderson has said that the new email viruses show less diversity than the old DOS versions. I disagree. But then, I would, wouldn't I? :-) The relation of types of antiviral and intrusion detection systems is good. Chapter nineteen, on protecting e-commerce systems, has good information but mixed in a bit of a grab bag: e-commerce is always a bit of a fuzzy topic. There is solid coverage of recent controversies in regard to copyright and privacy protection, in chapter twenty.

Part three turns to politics, management, and assurance. Chapter twenty one has a fascinating discussion of major issues in public policy. Management issues, in chapter twenty two, are presented in an interesting but generic manner. The discussion of system evaluation and assurance asks the usual question of how we know our systems are secure. In a sense, though, the subtitle of the book is wrong: much of the material points out how *not* to build dependable systems, and chapter twenty three is a bit disheartening. The conclusion, in chapter twenty four, is that we need more engineers and engineering.

Although the material is presented in a very formal way, the writing is usually quite readable, and the exceptional stilted passages are still accessible to the determined reader. On occasion, one could hope for additional explanations of some items that are mentioned briefly and passed over, but, by and large, one has to agree with Bruce Schneier's assessment, reprinted on the book jacket, that this is one of the most comprehensive works on security concepts that is available. The constant emphasis on how security protections have failed can be depressing, but the examination of the errors of others does provide the basis for better designs in the future.

copyright Robert M. Slade, 2002 BKSECENG.RVW 20021015
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

✦ REVIEW: "Network Intrusion Detection", Northcutt/Novak/ McLachlan

Rob Slade <rslade@sprint.ca>

Fri, 15 Nov 2002 07:44:13 -0800

BKNTINDT.RVW 20021009

"Network Intrusion Detection", Stephen Northcutt/Judy Novak/
Donald

McLachlan, 2001, 0-7357-1008-2, U\$45.00/C\$67.95/UK#34.99

%A Stephen Northcutt stephen@sans.org snorthcutt@hawaiian.net

%A Judy Novak

%A Donald McLachlan don_mclachlan@hotmail.com

%C 201 W. 103rd Street, Indianapolis, IN 46290

%D 2001

%G 0-7357-1008-2

%I Macmillan Computer Publishing (MCP)/New Riders

%O U\$45.00/C\$67.95/UK#34.99 800-858-7674 <http://www.newriders.com>

%P 430 p.

%T "Network Intrusion Detection: An Analyst's Handbook, Second
Ed."

The introduction for the first edition of this work was a bit
confusing.

The front matter for the second edition is much more so. The
only item

listed in the table of contents is the introduction, but, while
still

stating that the book is intended as a training aid and
reference for

intrusion detection analysts, it is much the smallest item of
the many at

the beginning of the book. There is a longish, and not very
clear, history

of the "shadow" program. In addition, there is a preface, which
meanders

around presenting opinions about various aspects of the Internet

and security. It does finally provide a rather interesting definition of intrusion detection; the purpose is to identify threats and make sure the network is hardened against them; but does not make clear what the book is for, or how it approaches the subject.

Chapter one is a basic overview of TCP/IP. The material is reasonable, albeit limited, but not exemplary. TCPdump is examined before TCP itself, in chapter two. Again, the content is informative, but there are definite gaps. Fragmentation uses, issues, and patterns in TCPdump are presented in chapter three. Chapter four does provide some idea of the use of ICMP (Internet Control Message Protocol), but not a comprehensive or clear one, and not in the stated introduction. The coverage of ICMP attacks is neither particularly lucid nor particularly complete. It does, however, furnish some convincing arguments for the use of stateful inspection.

Chapter five presents a few "normal" transactions that you might see in network traffic, and some that might indicate some type of attack. The material is interesting, but is not displayed in a structure that would make it useful to the reader. DNS (Domain Name Service) is explained in some detail in chapter six, although the attack and exploit coverage is terse. In chapter seven (chapter one, from the first edition), we are given some details of the TCP hijacking attack Kevin Mitnick launched against computers used by Tsutomu Shimomura. In fact we are given rather a lot of details,

and not a little C code, much of which is simply thrown out at us. The experienced UNIX network analyst and C programmer will, of course, have no difficulty with the material, and any reasonably experienced computer user will likely be able to find references in order to work through the real implications of the text. Late in the chapter there is a promise of explaining how to detect such an intrusion with two different systems: this promise is not fulfilled. The concept of filters and signatures is introduced in chapter eight, although the examples tend to be either system specific and heavily coded, or overly simplistic.

The initial section of chapter nine attempts to present a means for determining which events are important enough to record and analyze, and does not succeed very well. The latter portion, on considerations for intrusion detection system (IDS) architecture is much more useful. Chapter ten starts out with a look at a variety of attempts at interoperability between intrusion detection vendors (making me think of the bygone days of standardized virus signature files: the availability of standards is shown to be problematic) and then tenders some ideas about suspicious types of traffic, finishing with a few thoughts on database queries and data reduction. A number of IDSes are described in chapter eleven, although the level of detail, and even the general writeup structure, varies greatly.

Chapter twelve seems to be out of place: the prediction about the future

usually happens at the end of the book. Exploits, denial of service, and scan patterns are described in chapters thirteen, fourteen, and fifteen, repeating some of the material from chapters five and seven. Although interesting, not all of the content would be helpful to analysts or IDS administrators. Signatures related to the use of RPC (Remote Procedure Calls) as an attack tool are given in chapter sixteen. Chapter seventeen describes various options for filtering traffic for or with TCPdump. A "cracking" session, after a system has been penetrated, is presented in limited detail in chapter eighteen. In this case we are presented with a log of UNIX shell commands, and, rather ironically, a great deal more exegesis than is available in other sections (although the attempts at humour do confuse the issue, here and elsewhere in the book). A discussion of blackhat communities and resources has been added in this edition. A "detection" is outlined in chapter nineteen, but with a supremely anticlimactic ending: the summary admits that no reason for the anomalous traffic has been found.

Chapter twenty reviews some basic security topics, such as policy development and risk assessment, but in a very simplistic and terse fashion.

A number of possible responses to an intrusion are outlined in chapter twenty one. Chapter twenty two closes with suggestions on how to make a business case.

Those who need to know about intrusion detection should probably first look at Bace's (cf. BKNTRDET.RVW) or Amoroso's (cf. BKINTDET.RVW)

books, both
(somewhat annoyingly) titled "Intrusion Detection." Because of
the lack of
structure in the work, this volume is not usable as an overview
introduction
to the field, although the examples do contain a great deal of
informative
content: if you can dig it out. For those who do have the basic
concepts,
the material does provide numerous practical examples, and some
real-life
considerations for implementation.

copyright Robert M. Slade, 1999, 2002 BKNTINDT.RVW 20021009
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

<http://victoria.tc.ca/techrev> or <http://sun.soci.niu.edu/~rslade>



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

[ACM](#) Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 40

Tuesday 26 November 2002

Contents

- [Massive identity theft ring broken up](#)
[PGN](#)
- [Identity thieves strike eBay](#)
[Monty Solomon](#)
- [eBay sends plaintext password changes](#)
[Brian R. Neumann](#)
- [More on the Breeders Cup Pick-6 fix](#)
[PGN](#)
- [Windows quietly deletes Unix files](#)
[Doug McIlroy](#)
- [Patch slip-up raises security questions](#)
[Robert Lemos via Monty Solomon](#)
- [RIAA orders US Navy to surrender](#)
[Tim Finin via Dave Farber](#)
- [Re: Computer problem caused fatal pipeline rupture](#)
[Pekka Pihlajasaari](#)
- [Re: Readability of ATC displays at the London Area Control Centre](#)
[Peter B. Ladkin](#)
- [UK Publishes Security Requirements for e-Voting](#)
[Ian Cuddy](#)

- [Re: UK Publishes Security Requirements for e-Voting](#)
[Rebecca Mercuri](#)
 - [REVIEW: "The Privacy Papers", Rebecca Herold](#)
[Rob Slade](#)
 - [REVIEW: "Security, ID Systems and Locks", Joel Konicek/Karen Little](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Massive identity theft ring broken up

"Peter G. Neumann" <neumann@csl.sri.com>
Tue, 26 Nov 2002 19:17:11 PST

Identity theft has long been a concern in RISKS, where we have reported numerous cases. (For example, see my Illustrative Risks compendium, <http://www.csl.sri.com/neumann/illustrative.html> for browsing -- click on Identity Theft -- or .ps and .pdf for printing.)

In the early days, most of the cases involved one-on-one usurpation or masquerading as a particular individual, going back even further than the infamous Terry Rogan case. More recently, identity theft is becoming an industry in its own right, with massive acquisition of personal data sufficient to do serious damage on a large scale.

In the most recent cases, billed as probably the largest yet in the U.S., at least 30,000 people have been victimized as a result of an employee of a Long Island NY software company using a Ford Motor Credit Company code to access Experian. He obtained credit histories on people at the

request of
an identity theft ring operating in Brooklyn and the Bronx, to
whom he sold
that information for \$60 a pop. Together with information the
ring had
already obtained, this enabled them to clean out the victims'
bank accounts,
make bogus loans, max out existing and newly obtained credit
cards, etc.
This operation had apparently been going on for three years,
until -- in
response to numerous complaints -- the FBI was able to arrest
three people,
who appeared in court yesterday in Manhattan. Victims are asked
to call the
Federal Trade Commission hot line at 1-877-IDTHEFT, or access
www.ftc.gov.
[Source: Benjamin Weiser, *The New York Times*, beginning on the
front page,
26 Nov 2002; PGN-ed]

[Also noted by Alan P. Burke

[http://www.msnbc.com/modules/exports/ct_email.asp?/
news/839678.asp](http://www.msnbc.com/modules/exports/ct_email.asp?/news/839678.asp)

PGN]

Identity thieves strike eBay

Monty Solomon <monty@roscom.com>

Sat, 23 Nov 2002 22:40:50 -0500

Paul Festa, CNET News.com, 22 Nov 2002

When Deborah Fraser's credit card number was stolen, the thief
didn't use it
to buy a new car or a high-end laptop. Instead, the number was
used to buy
something potentially much more valuable--a domain name with the

word "ebay"
in it. In Fraser's case, that was the domain name "change-ebay.
com," a scam
Web site where an unknown number of eBay users may have been
tricked into
handing over their eBay username and password. ...

<http://news.com.com/2100-1017-966835.html>

✶ eBay sends plaintext password changes

"Brian R. Neumann" <brian@iswaycool.com>
Thu, 21 Nov 2002 14:28:17 -0700

I went to change my password for eBay after seeing the article
"What's real,
what's a scam? eBay users wondering",
(<http://www.msnbc.com/news/837882.asp>). There are significant
security
issues with eBay's password changing mechanism.

When a user changes their password using the method provided by
eBay, the
new password is sent over the Internet unencrypted! This is
especially bad
given that there are a large number of users changing passwords
given the
scammers and legitimate eBay change requests mentioned in the
above article.

EBay's security policy states that they always encrypt your
password. It's
true that they do perform a lightweight encryption for sign-in.
If you click
the "Secure sign in (SSL) " link on the login screen, your login
information
is passed via SSL. This is a good thing.

However, when you go to change your password, only the old password is encrypted. That is, YOUR NEW PASSWORD IS SENT UNENCRYPTED OVER THE INTERNET. You can log in securely once your password is set, but there's no way to securely set your password in the first place.

I've used a packet sniffer (Ethereal) to verify this. When you change your password via the method eBay provides you, (My eBay, Preferences, Change My password) and enter your information into the form, the following string is sent unencrypted over the Internet:

```
MfcISAPICommand=HandleNewPassword&from=###&userid=EBAYUSERNAME
&pass=ENCRYPTED_OLD_PASSWORD&npass=UNENCRYPTED_NEW_PASSWORD
&rpass=UNENCRYPTED_NEW_PASSWORD
```

Note that the username and new password are plainly visible. Encrypting the old password doesn't help at this point as it's about to be changed. We want the `_new_` one encrypted.

So exactly how can I feel secure on eBay?

An unscrupulous person at an ISP could take advantage of this by sending out faked ebay change-password e-mails and sniffing for password changes coming through. While the user would think everything is secured, they've just given away the new password. All kinds of personal data is then available within the user knowing the account has been compromised.

➤ **More on the Breeders Cup Pick-6 fix ([RISKS-22.33](#) and [39](#))**

RISKS List Owner <risiko@csl.sri.com>

Tue, 26 Nov 2002 16:07:01 PST

Subsequent analysis has now uncovered evidence that the Drexel frat buddies were apparently also able to collect on winning bets that had not yet claimed by the intended winners. (Over 14 years ago, we reported a lottery scam in [RISKS-6.77](#), 4 May 1988, in which someone with insider access to the Pennsylvania lottery system had fabricated a ticket for an unclaimed winning combination and attempted to collect before the expiration date. Unfortunately for him, he had used the wrong card stock from the would-be winning ticket -- each region had a different stock -- and thus he was caught.)

⚡ Windows quietly deletes Unix files

Doug McIlroy <doug@pierce.cs.dartmouth.edu>

Fri, 15 Nov 2002 12:38:43 -0500

How Windows deleted all the files in my Unix home directory.

My department has a typical distributed computing environment. Unix/Linux workstations anywhere can remotely mount the file systems from central Unix servers. By the magic of Samba, Windows systems can also remotely mount file systems from the same servers.

Not long ago, I logged into an NT machine that I'd never used before and was

pleased to find that I was already a registered user with my customary login directory. How convenient!

At logout, NT announced "Saving your settings" and stayed in that state for a remarkably long time. Back at Linux on my desk, I found my home directory curdled. The directory structure remained, but the files were gone throughout the directory tree. In their place was Microsoft boilerplate, such as "Favorites", to help me enjoy the good things of life like MSN and ESPN.

What had happened was that my NT account had mistakenly been configured to set a "roving profile" to be my remote home directory. In the course of "saving your settings", Windows evidently assessed the profile as weird and quietly cleaned it up. Thus Windows, which is usually reluctant to remove even one file locally without asking for confirmation, blasted away 6000 files on a remote machine with impunity. Why not? They were mere Unix files.

⚡ Patch slip-up raises security questions

Monty Solomon <monty@roscom.com>

Sat, 23 Nov 2002 23:11:32 -0500

Article by Robert Lemos, CNET News.com, 21 Nov 2002

The questionable handling of a fix for a recent widespread software

vulnerability has some administrators worried that developers can't be trusted to make security a top priority.

Last week, the Internet Software Consortium withheld the patch for a critical flaw in the domain name system (DNS) software from a large number of researchers, asking instead that each person send the organization an e-mail request in order to get the fix. The software, known as the Berkeley Internet Name Domain (BIND) program, performs a critical function as the address book for the Net. The delay, coupled with messages sent to several administrators urging them to pay to become part of an early-warning group run by the ISC, has some security experts worried that security is taking a backseat to secrecy and money. ...

<http://news.com.com/2100-1001-966666.html>

⚡ RIAA orders US Navy to surrender (via Dave Farber's IP)

Tim Finin <finin@cs.umbc.edu>
Mon, 25 Nov 2002 10:09:09 -0500

As seen in **The Register**:

RIAA orders US Navy to surrender
By Andrew Orłowski in San Francisco
<http://www.theregister.co.uk/content/6/28263.html>

In a timely reminder of who's really in charge here, the Recording

Industry Association of America (RIAA) has mounted a daring raid on the US

Navy.

Acting unilaterally at the behest of the RIAA, Navy officials confiscated

100 computers on suspicion of harboring illegally downloaded MP3s, The

Capital, an Annapolis, MD daily reports. A Naval official quoted confirms

the raid, adding that punishment ranges from "court martial to loss of

leave and other restrictions".

For the RIAA, there are no half measures: you're either with them, or

against them. So even if you're risking having your ass blown off for your

country, there's no mercy. ...

and in the Capital-Gazette Newspapers (Annapolis):

http://www.hometownannapolis.com/cgi-bin/read/live/11_23-19/NAV

and on slashdot:

<http://yro.slashdot.org/yro/02/11/24/2010223.shtml?tid=103>

Archives at: <http://www.interesting-people.org/archives/interesting-people/>

⚡ Re: Computer problem caused fatal pipeline rupture ([RISKS-22.36](#))

Pekka Pihlajasaari <pekka@data.co.za>

Tue, 26 Nov 2002 01:49:38 +0200

It is ingenuous to suggest that the Bellingham, Washington pipeline rupture was a result of a computer/software fault. The NTSB accident report clearly

attributes the failure to a combination of quality assurance lapses and operational errors.

Although some of these are related to the SCADA environment, they are

strongly overshadowed by:

- * multiple errors in the configuration and installation of a pressure relief valve upstream from the rupture,
- * physical damage by excavators to the pipeline during construction work, and
- * failure of the pipeline operator to act on inspection reports suggesting damage in the vicinity of the construction area.

The report states that had the pipeline not been damaged, the pressure surge allowed even by the faulty relief valve would most likely not have resulted in a rupture.

In this case, it seems that process-wide safety controls were in place and would have protected the pipeline from failure if the human factors of management and operational procedures had connected the reported system anomalies with a potential failure.

A classic combination of multiple independent failures occurring within sufficiently close proximity where any single event would not have compromised the overall system integrity.

Regulatory bodies will rightly bring up this incident when organisations involved in hazardous operations complain about the level of regulatory compliance procedures to which they are required to comply.

Pekka Pihlajasaari <pekka@data.co.za> Data Abstraction (Pty) Ltd

✈ Re: Readability of ATC displays at the London Area Control Centre

"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>

Tue, 19 Nov 2002 08:23:58 +0100

In [RISKS-22.09](#), Chris Brady reported on a BBC News article concerning readability problems of the controllers' display screens at the UK's New En-Route Centre (NERC), now the London Area Control Centre (LACC), for the London Flight Information Region, which came on-line in January 2002 after nearly a decade of development.

Brady said

"Obviously no-one thought to ask the controllers if they could actually read the screens clearly".

I replied in [Risks 22.12](#):

"On the contrary, controllers were evaluating and training on the system for at least two years before it went live in January, and it is public knowledge that they were very active with their feedback....."

I followed it up. It appears that the Head of Human Factors at National Air Traffic Services (NATS, the UK ATC service provider) identified a legibility problem with the size of text on the screens already in January 1997. It seems indeed that this problem was not adequately addressed before the NERC went live five years later, as the BBC and Brady reported.

The source of this information is a letter which appeared in The Ergonomist, the organ of The Ergonomics Society (<http://www.ergonomics.org.uk>) in June 2002 from Barry Kirwan, who was Head of Human Factors at NATS from September 1996 until March 2000.

The letter says that Kirwan and two other NATS ergonomists visited the NERC in January 1997 and "identified a number of problems, including a significant one with the legibility of the text on the screens. Legibility... is a function of a number of factors.... but the main problem seemed to be simply the size of text, given the viewing distance afforded by the work-station layout. Since this text referred to all of the main information available to the controller, including flight levels, we considered this an important issue."

The letter goes on to describe Kirwan's attempts to have the issue addressed, and some organisational difficulties he encountered. He considers his group's "impact on the NERC interface" to be "relatively unsuccessful" and suggests some organisational reasons for it. Concerning the issue Brady and I discussed, he says "There was also advice from controllers, but some controllers' advice was seen as more valid than others'."

I recommend reading the letter in full.

Peter B. Ladkin, University of Bielefeld, <http://www.rvs.uni-bielefeld.de>

UK Publishes Security Requirements for e-Voting

"Ian Cuddy" <ic@egovmonitor.com>

Thu, 21 Nov 2002 19:54:35 -0000

[You may reproduce this article on condition that
"eGov monitor Weekly
www.egovmonitor.com/newsletter/signup.asp" is included at the
top and
"Copyright KAM 2002" is included at the bottom.
Ian Cuddy, Chief Editor, eGov monitor www.egovmonitor.com
T 020 7384 1551 F 020 7384 2551 E ic@egovmonitor.com]

UK Publishes Security Requirements for e-Voting (eGov monitor
Weekly)

www.egovmonitor.com/newsletter/signup.asp

The UK Government has released a new set of security
requirements that will
form the baseline for all future implementations of electronic
voting
systems.

This first statement of technical requirements will apply to the
second
phase of electoral modernisation pilots taking place in local
government
elections next May. The document was drawn up following an
"urgent"
consultation with IT suppliers earlier this year.

The security requirements are considered by the Government to
represent the
standard by which security measures for e-voting can be
considered "adequate
and acceptable". This working definition is expected to change
as local
councils and their IT partners gain more experience of the
practical
arrangements of running e-voting systems.

The criteria for the main security controls have been based on a

"best-of-breed" set of principles compiled from various sources, including those used by the California Internet Voting Task Force. These principles - dealing with issues such as system reliability, voter authenticity and data integrity - have been translated into 15 high-level "control objectives", such as guaranteeing the confidentiality of the vote until it is counted. If fully met, this should ensure that threats associated with the use of e-voting systems and services are properly countered, the document claims.

The actions necessary to implement each of the 15 control objectives form the technical security requirements, outlining, for example, the mechanisms, systems or procedure that should be in place.

The document does not explain how this will be achieved.

<http://www.local-regions.odpm.gov.uk/elections/pdf/evoting.pdf>

- Ian Cuddy, eGov monitor Weekly, Copyright KAM 2002

[Re: UK Publishes Security Requirements for e-Voting \(Cuddy, R-22.40\)](#)

"Notable Software" <notable@mindspring.com>

Sat, 23 Nov 2002 18:44:50 -0500

The United Kingdom and other European countries have begun initiatives to convert all or part of their voting to electronic balloting (kiosk/DREs and/or Internet-based) systems. Europe appears to be rushing ahead to

deploy computer voting technologies with serious sociological and technological downsides, such as lack of auditability, and increased opportunities for vote selling, monitoring, coercion, and denial of service attacks. During mid-October, 2002 I visited England, on the invitation of the Foundation for Information Policy Research, to meet with and brief members of the UK Cabinet and Parliament regarding this subject, and to provide technical lectures at the Royal Academy of Engineering and Cambridge University. My comments to the Cabinet are on the Cabinet Office's official website at <http://www.edemocracy.gov.uk> -- a mildly corrected version is posted *here*. I also formally submitted an additional follow-up comment as part of their "In the Service of Democracy" consultation, which explains why Internet voting is not appropriate for UK democratic elections.

[Links can be found on Rebecca's Web site
www.notablessoftware.com/evote.html

Her testimony and comments should be looked at to gain some perspective on the scope and extent of the problem of implementing Internet and electronic voting. In the light of that testimony, the uk decision to proceed seems very RISKY indeed. PGN]

🔥 REVIEW: "The Privacy Papers", Rebecca Herold

Rob Slade <rslade@sprint.ca>

Wed, 20 Nov 2002 08:03:00 -0800

BKPRVPAP.RVW 20020926

"The Privacy Papers", Rebecca Herold, 2002, 0-8493-1248-5, U
\$69.95

%A Rebecca Herold

%C 920 Mercer Street, Windsor, ON N9A 7C2

%D 2002

%G 0-8493-1248-5

%I Auerbach Publications

%O U\$69.95 +1-800-950-1216 auerbach@wgl.com orders@crcpress.com

%P 679 p.

%T "The Privacy Papers: Managing Technology, Consumer,
Employee,
and Legislative Actions"

The preface asserts that this volume is intended as an
introduction to
privacy for C-level executives. (I assume that means "Chief"
executive officers, security officers, information officers, and
the
like, rather than referring to the grades they made in school.)
This
assertion is a bit odd, both in terms of the enormous size of the
volume, and in terms of the statement, in the foreword, that the
papers are included based on the editors personal choice.

The introduction gives a historical look at early US privacy law.

Part one deals with business organization issues, including
papers on the
privacy of employee e-mail (case studies that are often
unresolved), e-mail
pornography policy (have one), computer forensics and privacy
(almost no
content), policies for secure personal data (random security
topics),
security awareness (good program, but generic and not tailored
for privacy),
the case for privacy (vague thoughts, no case), attorney-client
privilege
and electronic data transmission (careless use of communications
technology
may void privilege), computer crime and analysis of computer

evidence (you can get evidence from computers), a tale of two spies (spies may use computers), (US) federal laws affecting information systems auditors (more politics than details), computer forensics (*extremely* vague), the dangerous precedent set in the use of electronic identifiers (various cases linked *only* by the fact that *none* have been tested in court and therefore no precedents have been set), jurisdictional issues (almost irrelevant to privacy), anonymity on the net (generic), erosion of confidentiality (anecdotal reports), export regulations for cryptography (irrelevant to privacy), security awareness training (irrelevant), security standards (irrelevant to privacy), chief medical information officers (oddly irrelevant), information security management in healthcare (interesting and detailed), criminal activity on the Internet (clear but not much detail), identify theft (interesting but undetailed), identity theft (US-centric and not always helpful), obtaining information from ISPs (information service providers) (detailed content on a complex topic).

Part two reviews tools and related technology. The first paper not only does not advise on its stated topic, selecting a cryptographic system, but it demonstrates essentially no understanding of cryptographic concepts, and a truly astonishing range of errors. (There definitely are inherent differences between symmetric and asymmetric encryption, asymmetric encryption does not use digital signatures, but provides for them, and the electronic codebook mode of DES [Data Encryption Standard] is not less able to provide authentication than the chaining modes.) Other essays deal with

new paradigms for steganography (pointless), cookies and web bugs (a brief and limited apologia), online profiling (a political report on online business), intrusion detection systems (a review of a conference on the topic), Internet acceptable use policies (banal and unhelpful), ethics and the Internet (a brief take, only marginally about privacy), security of wireless LANs (long out of date), customer relationship management and data warehousing (little about privacy), anonymity, privacy, and trust (brief and random), Web certification (promotional piece for ICSA Labs), and an exhortation to get people to sign a confidentiality agreement.

Part three is about US laws and issues. The pieces in this section are primarily either documents prepared by government departments, or prepared testimony before legislative committees (and sometimes both).

There is a FAQ (Frequently Asked Questions list) on the HIPAA (Health Insurance Portability and Accountability Act) privacy rule prepared by the Department of Health and Human Services, testimony on HIPAA, a non-detailed description of the provisions of the Financial Services Modernization Act, a list of US laws with privacy provisions and another of proposed laws as of July 2001, testimony about privacy in wiretap laws, and a report on the Carnivore system.

Part four turns to international laws and issues. The European Union directive on privacy is attacked as a barrier to trade, there is a

detailed (but not very interesting or helpful) review of the EU directive and how it is implemented by some of the member states, a Department of Commerce description of the Safe Harbor program, and a list of international privacy laws.

While isolated articles in this volume are interesting, the reader would have to be rather ignorant about privacy issues in order to get much out of the text overall.

copyright Robert M. Slade, 2002 BKPRVPAP.RVW 20020926
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com
<http://victoria.tc.ca/techrev/~rslade> or <http://sun.soci.niu.edu/~rslade>

REVIEW: "Security, ID Systems and Locks", Joel Konicek/ Karen Little

Rob Slade <rslade@sprint.ca>
Thu, 14 Nov 2002 07:51:18 -0800

BKSIDSAL.RVW 20021012

"Security, ID Systems and Locks", Joel Konicek/Karen Little,
1997,

0-7506-9932-9, U\$39.99

%A Joel Konicek

%A Karen Little

%C 225 Wildwood Street, Woburn, MA 01801

%D 1997

%G 0-7506-9932-9

%I Butterworth-Heinemann/CRC Press/Digital Press

%O U\$39.99 800-272-7737 www.bh.com/bh/ dp-catalog@bh.com

%P 244 p.

%T "Security, ID Systems and Locks: The Book on Electronic
Access
Control"

This is an easy to read, illustrated, quick guide to a lot (not
all)
of physical security.

Chapter one introduces electronic access control, primarily
access
cards and sensor systems. Then we got back to ancient history:
chapter two looks at old fort and defensive technology, which
lives on
both in concepts and in terms still used. Credentials, such as
identification and authentication systems, cards, and
biometrics, are
reviewed in chapter three. Chapter four deals with barriers like
doors and locks, concentrating on electronic systems. Oddly, the
issue of power failure is not addressed, although there is a good
section on fire exits. Sensors, as the input part of an alarm or
control system, are discussed in chapter five. There is a simple
guide to (mostly Wintel) computers in chapter six. Cabling and
other
technology that may be used for communications in a security
system is
examined in chapter seven. Systems design, in chapter eight,
scrutinizes a variety of aspects, some of which have been
previously
covered. Chapter nine, entitled system integration, is actually
more
system design. Chapter ten looks at how a number of companies
are
using electronic access.

While limited to electronic systems, the book is a very
reasonable
guide to a lot of physical security technology.

copyright Robert M. Slade, 2002 BKSIDSAL.RVW 20021012
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

[ACM](#) Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 41

Thursday 5 December 2002

Contents

- [Understanding the Windows 2000 EAL4 Evaluation](#)
[Jonathan S. Shapiro](#)
- [L.A. woman gets prison in counterfeit software ring](#)
[Monty Solomon](#)
- [NSF Fastlane Exposes PINs](#)
[Geoff Kuenning](#)
- [UK Government under digital attack: security breaches revealed](#)
[Ian Cuddy](#)
- [Internet eBay auction scam](#)
[NewsScan](#)
- [Re: eBay sends plaintext password changes](#)
[George C. Kaplan](#)
- [Re: Patch slip-up raises security questions](#)
[Fred Cohen](#)
- [REVIEW: "XML Security", Blake Dournae](#)
[Rob Slade](#)
- [REVIEW: "A Guide to Business Continuity Planning", James C. Barnes](#)
[Rob Slade](#)
- [CFP: Workshop on Investigation & Reporting of Incidents & Accidents](#)
[C. Michael Holloway](#)

● [Info on RISKS \(comp.risks\)](#)

✶ Understanding the Windows 2000 EAL4 Evaluation, Jonathan S. Shapiro

"Peter G. Neumann" <neumann@csl.sri.com>

Wed, 27 Nov 2002 7:11:48 PST

Understanding the Windows EAL4 Evaluation
Jonathan S. Shapiro, Johns Hopkins University Information
Security Institute

"Jonathan S. Shapiro" <shap@eros-os.org>

<http://eros.cs.jhu.edu/~shap/NT-EAL4.html>

[Via Bruce Schneier's Crypto-Gram (courtesy of Paul Walczak)]

By now, you may have heard that Microsoft has received a Common
Criteria
certification for Windows 2000 (with service pack 3) at
Evaluation Assurance
Level (EAL) 4. Since a bunch of people know that I work on
operating system
security and on security assurance, I've received lots of notes
asking "What
does this mean?" On this page I will try to answer the question.
For the
impatient the answer is:

Security experts have been saying for years that the security of
the Windows
family of products is hopelessly inadequate. Now there is a
rigorous
government certification confirming this.

Since that's a pretty strong statement, bear with me while I try
to explain
it in plain English.

How a Security Purchase Should Work (In Abstract)

At the risk of telling you something you already know, here is

how a purchaser ought to proceed when buying a security product:

- * Assess your needs. Determine what your requirements are.
- * Decide which product you are most confident will meet those needs.
- * Buy and deploy it.

Each of these is potentially an involved process, and most customers don't have the expertise to do them effectively. Even if you did, Microsoft (or any other vendor) isn't likely to let you examine their code and design documents in order to evaluate their product.

The purpose of the Common Criteria process is to develop standard packages of commonly found requirements (called Protection Profiles) and have a standard process of independent evaluation by which an expert evaluation team arrives at a level of confidence for some particular software product.

As a customer, this makes your life simpler, because you can compare your needs against existing requirements constructed by experts and then see how well the software you are buying meets those requirements. Security requirements are fairly hard to write down correctly, but if the resulting document is annotated properly they aren't all that hard to understand.

Obviously, if you don't know your needs (requirements) you don't stand much of a chance of getting them met. Likewise, if you don't know what requirements a software product was evaluated against, the evaluation result isn't terribly useful to you in practical terms.

How Common Criteria Works

>From the customer perspective, a Common Criteria evaluation has two parts:

A standardized requirements specification called a Protection Profile that says what the system is supposed to do. Sometimes there will be more than one of these -- usually a general baseline protection profile and then some others describing additional, specialized requirements.

An evaluation rating. This is basically an investigation by well-trained experts to determine whether the system actually meets the requirements specified in the protection profile(s). The result of the evaluation is an "Evaluation Assurance Level" which can be between 1 and 7. This number expresses the degree of confidence that you can place in the system.

In order to understand the result of an evaluation, you need to know both the evaluation result, which will be a level between EAL1 and EAL7, and the protection profile (the requirements that were tested). Given two systems evaluated against the same protection profile, a higher EAL rating is a better rating provided the requirements meet your needs.

Knowing that a product has met an EAL4 evaluation -- or even an EAL7 evaluation -- tells you absolutely nothing useful. It means that you can have some amount of confidence that the product meets an unknown set of requirements. To give a contrived example, you might need a piece of software that always paints the screen black. I might build a

piece of software that paints the screen red with very high reliability, and get it evaluated at EAL4. Obviously my software isn't going to solve your problem.

The Windows 2000 Evaluation

Microsoft sponsored an evaluation of Windows 2000 (with Service Pack 3 and one patch) against the Controlled Access Protection Profile (plus some enhancements) and obtained an EAL4 evaluation rating. This is most accurately written as "CAPP/EAL4".

Problem 1: The Protection Profile

The Controlled Access Protection Profile (CAPP) standard document can be found at the Common Criteria website. Here is a description of the CAPP requirements taken from the document itself (from page 9):

The CAPP provides for a level of protection which is appropriate for an assumed non-hostile and well-managed user community requiring protection against threats of inadvertent or casual attempts to breach the system security. The profile is not intended to be applicable to circumstances in which protection is required against determined attempts by hostile and well funded attackers to breach system security. The CAPP does not fully address the threats posed by malicious system development or administrative personnel.

Translating that into colloquial English:

Don't hook this to the Internet, don't run e-mail, don't install software

unless you can 100% trust the developer, and if anybody who works for you turns out to be out to get you you are toast.

In fairness to Microsoft, CAPP is the most complete operating system protection profile that is presently standardized. This may be the best that Microsoft can do, but it is very important for you as a user to understand that These requirements are not good enough to make the system secure. It also needs to be acknowledged that commercial UNIX-based systems like Linux aren't any better (though they are more resistant to penetration).

Note that the "Don't install software" part means that you probably shouldn't install a word processor. On several occasions Microsoft has unintentionally shipped CD's with viruses on them. A CD with a virus qualified as "malicious system development."

Problem 2: The Evaluation Assurance Level

Having described the requirements problem, I now need to describe the problem of the EAL4 evaluation assurance level that Windows 2000 received.

As I mentioned before, EAL levels run from 1 to 7. EAL1 basically means that the vendor showed up for the meeting. EAL7 means that key parts of the system have been rigorously verified in a mathematical way. EAL4 means that the design documents were reviewed using non-challenging criteria. This is sort of like having an accounting audit where the auditor checks that all of your paperwork is there and your business practice standards are

appropriate, but never actually checks that any of your numbers are correct.

An EAL4 evaluation is not required to examine the software at all.

An EAL4 rating means that you did a lot of paperwork related to the software process, but says absolutely nothing about the quality of the software itself. There are no quantifiable measurements made of the software, and essentially none of the code is inspected. Buying software with an EAL4 rating is kind of like buying a home without a home inspection, only more risky.

The Bottom Line for Windows 2000

In the case of the CAPP protection profile, there actually isn't much point to doing anything better than a low-confidence evaluation, because the requirements set itself is very weak. In effect, you would be saying "My results are inadequate, but the good news is that I've done a lot of work so that I can be really sure that the results are inadequate."

In the case of CAPP, an EAL4 evaluation tells you everything you need to know. It tells you that Microsoft spent millions of dollars producing documentation that shows that Windows 2000 meets an inadequate set of requirements, and that you can have reasonably strong confidence that this is the case.

Conclusion

Security isn't something that a large group can do well. It is something

achieved by small groups of experts. Adding more programmers and more features makes things worse rather than better. Microsoft has been adding features demanded by their customers for a very long time.

It is possible to do much better. EROS, a research operating system that we are working on here in the Systems Research Laboratory at Johns Hopkins University, should eventually achieve an EAL7 evaluation rating, and is expected to provide total defense against viruses and malicious code. It won't be compatible, because the most important security problems in Windows and UNIX are design problems rather than implementation problems. In fact, none of the viable research efforts toward secure operating systems are compatible with existing systems.

It remains to be seen whether EROS or one of the other attempts to build secure operating systems will prevail, but better solutions are coming.

[We somehow keep coming back to electronic voting machines in RISKS. The 2002 FEC "Voting System Standards" document says that COTS software does not have to be inspected if it is used in the construction of a voting system. So any voting machine using Win2K can claim Common Criteria compliance, even though it may be riddled with security flaws! PGN]

⚡ L.A. woman gets prison in counterfeit software ring

Monty Solomon <monty@roscom.com>

Sat, 23 Nov 2002 19:10:50 -0500

A Los Angeles woman was sentenced on 22 Nov 2002 to nine years in prison and ordered to pay \$11 million in restitution for her role in one of the largest counterfeit software cases in U.S. history. The sentence imposed on 52-year-old Lisa Chen by Superior Court Judge Ronni MacLaren was the longest prison term for a first-time conviction on software piracy, prosecutors said. ... [Reuters, 22 Nov 2002]

- <http://finance.lycos.com/home/news/story.asp?story=30082290>

NSF Fastlane Exposes PINs

Geoff Kuenning <geoff@cs.hmc.edu>

Wed, 4 Dec 2002 12:09:33 -0800 (PST)

Today is the deadline for submitting reference letters for applicants for NSF graduate fellowships, and the quickest way to do so is through FastLane.

Most of their system is relatively friendly, but when you begin working on a new student, you are asked for a PIN (actually, it's a password) and the following message is displayed:

Your PIN will be used to identify you for future access to your Reference Report and to protect it from unauthorized access.

Note that it does **not** give any information about how long the

PIN might be necessary, whether it will be shared among other students you are creating references for, or what might be a good algorithm for selecting a PIN. Lacking such, and being in a hurry, I foolishly chose one of my standard passwords that I use for a number of moderately secure applications.

Imagine my surprise when a few moments later I received a cleartext e-mail telling me the PIN I had chosen! Nowhere on the Web page does the NSF hint that the "secret" value you are typing will immediately be mailed to you in cleartext. Since many people manage password explosion by reusing passwords, this could potentially expose the password to much more critical things than reference letters.

Geoff Kuenning geoff@cs.hmc.edu <http://www.cs.hmc.edu/~geoff/>

🚨 UK Government under digital attack: security breaches revealed

"Ian Cuddy" <ic@egovmonitor.com>
Mon, 2 Dec 2002 19:48:02 -0000

By Ian Cuddy, eGov monitor Weekly
www.egovmonitor.com/newsletter/signup.asp

UK Government departments have experienced more than 9,000 "digital attacks" on their IT systems so far this year, it has emerged.

The security threat was revealed in Ministers' responses to a

series of parliamentary questions tabled by Labour Party backbencher Brian White MP.

Over half of the incidents were directed towards the Cabinet Office and its agencies, which during 2002 reported some 5,857 attacks, with 1,167 of these occurring in October alone. Douglas Alexander, the Minister for e-Transformation, said that none of the events had resulted in "compromise, loss or damage to any information held on the systems".

By contrast, the Treasury, the Foreign and Commonwealth Office, Department for Education and Skills and the Department for Culture, Media and Sport said they had not detected a single attack on their systems this year. The Treasury admitted, however, it had discovered in June that an external website had been attacked while it was still under construction.

The Ministry of Defence confirmed that 10 computer hacking incidents, including a website defacement, had taken place since January although none of these, it said, had a "significant" impact on military operations or core Defence business.

The Home Office reported no hacking attempts this year but said that around 2,500 attacks involving computer viruses had been detected. In the same period the Department for Environment, Food and Rural Affairs said it had experienced 564 attacks which were all blocked by its security measures.

The Department for International Development also disclosed a series of incidents where viruses had infected internal computers. In

April the destructive Elkern virus slipped past the Department's defences and spread to 500 PCs - about one in six computers - before it was stopped. The DFID is currently conducting a review of anti-virus arrangements which is expected to be completed and put into effect by the end of this month.

Ian Cuddy, Chief Editor, eGov monitor www.egovmonitor.com
T 020 7384 1551 F 020 7384 2551 E ic@egovmonitor.com

Internet eBay auction scam

"NewsScan" <newsscan@newsscan.com>
Thu, 05 Dec 2002 09:15:16 -0700

A 27-year-old Los Angeles man, Chris Chong Kim, has been charged with defrauding eBay buyers on six continents who had purchased computer equipment from him but never received delivery of the products they had purchased. The criminal complaint against Kim details losses of \$453,000 to 26 U.S. customers and to eBay and Bank of America. If convicted, Kim will face a penalty of up to 24 years in prison. [Reuters/*USA Today*, 4 Dec 2002; NewsScan Daily, 5 December 2002]

http://www.usatoday.com/tech/news/2002-12-04-ebay-scam_x.htm

Re: eBay sends plaintext password changes (B.R.Neumann, [RISKS-22.40](#))

"George C. Kaplan" <gckaplan@enceladus.Net.Berkeley.EDU>

Wed, 27 Nov 2002 09:58:58 -0800 (PST)

: An unscrupulous person at an ISP could take advantage of this
by sending out
: faked eBay change-password e-mails and sniffing for password
changes coming
: through.

There are lots of scenarios that wouldn't even require any help
from ISP
insiders. Anyone could do this at a public wireless hotspot,
for example.

George C. Kaplan, Communication & Network Services, University of
California at Berkeley 1-510-643-0496 gckaplan@ack.berkeley.
edu

✶ Re: Patch slip-up raises security questions (Solomon, [RISKS-22.40](#))

Fred Cohen <fc@all.net>

Wed, 27 Nov 2002 06:45:11 -0800 (PST)

> [Re: BIND] The delay, coupled with messages sent to several
administrators
> urging them to pay to become part of an early-warning group
run by the
> ISC, has some security experts worried that security is taking
a backseat
> to secrecy and money. ...

Sounds more like a shakedown to me. If this story is accurate,
the
consortium appears to be threatening other entities with
collapse of their
infrastructure unless they pay the consortium for the

information on how to
be safe. This is, in many ways, similar to what the AtStake
folks used to
do. They would create vulnerability exploit scripts and then
sell the
defenses to the vendors prior to making the attack script
available for
free.

I guess it's time to move away from BIND to a source that is
truly open,
and perhaps one that is really secure. Which brings up point
2. BIND has
been around for many many years. It seems to me that the effort
put into
patching and reworking this software long ago exceeded the cost
of doing a
trusted version. If it is in the national interest to secure
this
infrastructure, when will the government act in the common
defense and
provide properly skilled people with the \$s to do these jobs
right once and
for all?

Fred Cohen <http://all.net/> fc@all.net fc@unhca.com tel/fax:
925-454-0171
Fred Cohen & Associates - University of New Haven - Security
Posture

⚡ REVIEW: "XML Security", Blake Dournaee

Rob Slade <rslade@sprint.ca>
Tue, 3 Dec 2002 07:42:56 -0800

BKXMLSCR.RVW 20021003

"XML Security", Blake Dournaee, 2002, 0-07-219399-9, U\$59.99

%A Blake Dournaee
%C 300 Water Street, Whitby, Ontario L1N 9B6
%D 2002
%G 0-07-219399-9
%I McGraw-Hill Ryerson/Osborne
%O U\$59.99 800-565-5758 fax: 905-430-5020
%O [http://www.amazon.com/exec/obidos/ASIN/0072193999/
robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/0072193999/robsladesinterne)
%P 379 p.
%T "XML Security"

Chapter one is an outline of the book. The differences between symmetric and asymmetric cryptography are given in chapter two, which

provides a good treatment of the basics, although there are odd additions of extraneous details. The XML primer, in chapter three,

follows the all-too-common practice of describing syntax rather than

function, but the explanation of document parts is useful. The syntax

of XML digital signatures, and a brief mention of canonicalization,

makes up chapter four. Part two of the introduction to signatures is

in chapter five, which concentrates on canonicalization, but does not

present this important concept clearly. Chapter six provides some

examples, although neither the problems nor the solutions are defined

well. The elements of XML encryption are listed in chapter seven.

Chapter eight is a promotion for an RSA product. The elements of the

XML key management specifications are given in chapter nine.

While the syntax of various XML operations is provided properly, the

book fails to provide the newcomer to the field with any understanding

of the uses or limitations of the XML security provisions.

copyright Robert M. Slade, 2002 BKXMLSCR.RVW 20021003
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

<http://victoria.tc.ca/techrev/~rslade> or <http://sun.soci.niu.edu/~rslade>

★ REVIEW: "A Guide to Business Continuity Planning", James C. Barnes

Rob Slade <rslade@sprint.ca>
Tue, 19 Nov 2002 07:47:24 -0800

BKAGTBCP.RVW 20020922

"A Guide to Business Continuity Planning", James C. Barnes, 2001,
0-471-53015-8, U\$35.00

%A James C. Barnes

%C 5353 Dundas Street West, 4th Floor, Etobicoke, ON M9B 6H8
%D 2001

%G 0-471-53015-8

%I John Wiley & Sons, Inc.

%O U\$35.00 416-236-4433 fax: 416-236-4448

%P 174 p.

%T "A Guide to Business Continuity Planning"

Chapter one is an introduction, and also introduces us to a characteristic of the book: enormous tables with little apparent purpose. Table 1.1 is a list, by country, of regulatory agencies that may have something to require from you in the way of business continuity planning (BCP). The table is stated to be for motivational use, but does point out some BCP ideas or policies. There is also a rather innocent sounding mention that the book is written from the perspective of a consultant: this fact is more significant than the

reader may realize. For project foundation, chapter two does not give the usual advice to get management on-side and build a broadly based team, but concentrates on costing, expanding, and selling consulting services. (There are confusing areas: having presented one questionnaire, the text tells you to use results from "the two." Some items (such as the advice to use a month's worth of invoices to estimate rate of consumption of supplies) are helpful, but a lot of space seems to be wasted (on things like pages of fake employee and customer data--and a month's worth of supply invoices). The list of threats, consequences, and preventive measures is more than usually detailed (and listed twice), in chapter three, but the discussion of business impact analysis (BIA) itself is *extremely* terse. Chapter four's initial material on strategy selection is quite confused. The example RFP (Request For Proposal) for business continuity services does have some good points, but the pages of lists of specific PCs to be provided seem pointless. Later details are brief, but reasonable. Plan development, in chapter five, assumes multiple teams and, again, has some good points (the provision for leadership succession), but the lists become too specific in many places (does the top level emergency management team really all need to do CPR?) There is almost no general discussion of testing and maintenance in chapter six.

The book is not necessarily wrong, but only has enough real material for a good magazine article.

copyright Robert M. Slade, 2002 BKAGTBCP.RVW 20020922
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

<http://victoria.tc.ca/techrev> or <http://sun.soci.niu.edu/~rslade>

✦ CFP: Workshop on Investigation & Reporting of Incidents & Accidents

"C. Michael Holloway" <c.m.holloway@larc.nasa.gov>

Tue, 03 Dec 2002 08:30:06 -0500

The following Workshop should be interesting to many RISKS readers.

C. Michael Holloway, Senior Research Engineer, NASA Langley Research Center

General Chair IRIA 2003 <<http://shemesh.larc.nasa.gov/iria03/>>
Workshop on Investigation & Reporting of Incidents & Accidents

IRIA 2003 (First Call for Papers)

<<http://shemesh.larc.nasa.gov/iria03/>>

Mirror at <<http://www.logicteacher.com/iria03/>>

Deadline: 28 March 2003

The 2nd Workshop on the Investigation and Reporting of Incidents and

Accidents (IRIA03) will be held 16 - 19 September 2002, at the Radisson

Fort Magruder Hotel & Conference Center in Williamsburg, Virginia, United States.

Incident and accident investigation and reporting systems play a primary role in the safety of many industries across the globe. These systems are

diverse; the practices and techniques that have been developed within one industry are seldom shared by those in other areas. Similarly, techniques that have been developed within one national industry are often different from those that are used in the same industry in other countries. These observations have considerable practical consequences. It can be difficult or impossible to exchange data between these many diverse systems.

Similarly, it can be difficult to ensure that 'best practices' are effectively transferred between industries and between national systems.

This workshop is intended to provide a forum for the exchange of information about incident and accident investigation and reporting systems in many different application domains, including but not limited to aviation, automotive industry, chemical process industry, healthcare, military systems, marine systems, the rail industry, and nuclear applications.

Topics of interest include, but are not limited to, the following:

- o incident and accident causal analysis techniques
- o investigatory techniques, particularly for gathering of evidence
- o forensic software engineering and techniques for analyzing software failure
- o presentation and dissemination of safety-related information and recommendations
- o integrating incident and accident recommendations into broader risk

analysis and assessment

- o the integration of human factors, system engineering, and management concerns

- o data mining and trending techniques for incident and accident data

- o validation and the monitoring of incident and accident investigation and reporting systems

- o field studies in the application of incident and accident reporting

- o studies of the rhetoric of incident and accident reports

- o tools for supporting incident and accident investigation and reporting

Authors should submit full papers not exceeding 6000 words to the Program

Committee Chair, Barry Strauch <STRAUCB@ntsb.gov>, by 28 March 2003. Papers should consist of original work not submitted elsewhere.

Electronic submissions are encouraged. PDF is the preferred format, but other formats will be accepted for initial submissions.

Authors will be notified of the Program Committee's decision by 23 May

2003. Authors of accepted papers will be given instructions about the required format of the final papers.

Revised final versions of all papers must be received by 14 July 2003 for

inclusion in the Workshop Proceedings, which will be published as a NASA

Conference Publication. Final papers will also be published on the workshop web site.

General Chair: C. Michael Holloway, NASA Langley Research Center

Program Committee Chair: Barry Strauch, National Transportation Safety Board

Program Committee Members (with more to be added)

D. Busse, Microsoft

E. Byrne, NTSB

F. Chandler, NASA

J. Davies, U. Calgary

K. Hanks, U. Virginia

M. Holloway, NASA

C. Johnson, U. Glasgow

J. Knight, U. Virginia

P. Ladkin, U. Bielfeld

N. Leveson, M.I.T.

R. Mumaw, Boeing

M. O'Leary, British Airways

T. Panontin, NASA

J. Stoop, Tech. Univ. of Delft

B. Strauch, NTSB

T. van der Schaaf, Eindhoven U. of Tech.

For the latest information about IRIA03, visit the web site at <http://shemesh.larc.nasa.gov/iria03/>. If you have any problems with that address, try the mirror at <http://www.logicteacher.com/iria03/>

C. Michael Holloway, Senior Research Engineer, NASA Langley Research Center

General Chair IRIA 2003 <http://shemesh.larc.nasa.gov/iria03/>
Workshop on Investigation & Reporting of Incidents & Accidents



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

[ACM](#) Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 42

Weds 11 December 2002

Contents

- [A little bit of anti-porn filtering can go a long way](#)
[NewsScan](#)
- [Ironic filtering](#)
[Ray Dillinger in rec.humor.funny via Dawn Cohen](#)
- [Impostor eBay site set up to steal credit info](#)
[NewsScan](#)
- [Feds raid Ptech looking for al Qaeda link](#)
[PGN](#)
- [Web Surfers: What could they be thinking?](#)
[NewsScan](#)
- [UK police offer anonymity to cybercrime victims](#)
[PGN](#)
- [Anti-worm "throttling"](#)
[Rob Slade](#)
- [More on dangers of spelling correctors](#)
[Gene Spafford](#)
- [Your empty mailbox is full](#)
[Peter Kaiser](#)
- [Re: Windows 2000 EAL4 Evaluation](#)
[Rick Smith](#)

- [REVIEW: "VPNs: A Beginner's Guide", John Mairs](#)
[Rob Slade](#)
 - [REVIEW: "IPSec: Securing VPNs", Carlton Davis](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ A little bit of anti-porn filtering can go a long way

"NewsScan" <newsscan@newsscan.com>

Wed, 11 Dec 2002 09:54:22 -0700

"A little bit of filtering is O.K., but more isn't necessarily better," says Vicky Rideout, vice president of the Henry J. Kaiser Family Foundation, which conducted a study showing that when anti-pornography Internet filtering software is set at a low level of restriction, it's just as effective as when it is set a high level, and is far less likely to prevent searchers from reaching bona fide health sites. But some observers, such as Judith F. Krug of the American Library Association, think that filters are such blunt instruments that they should not be used at all in public institutions: "Filters are just fine for parents to use at home. They are not appropriate for institutions that might be the only place where kids can get this information." The filtering programs generally block any references to sex-related terms; examples given by the report include such subjects as safe sex, condoms, abortion, jock itch, gay, and lesbian. [*The New York Times*, 11 Dec 2002; NewsScan Daily, 11 December 2002]

<http://partners.nytimes.com/2002/12/11/technology/11FILT.html>

✶ Ironic filtering (Ray Dillinger in rec.humor.funny)

"Dawn Cohen" <COHEND@wyeth.com>

Fri, 06 Dec 2002 09:38:42 -0500

Freedom of sXYZch
bear@sonic.net (Ray Dillinger)

(smirk, computers)

"Congress shall make no law abridging the freedom of sXYZch, or the right of the people peaceably to XYZemble, and to peXYZion the government for a redress of grievances."

-- but your ISP might.

[This item also noted by Carl Ellison. I changed the three-X strings in Ray's original piece to YXZ, in order to avoid having this issue ex-filtrated. PGN]

✶ Impostor eBay site set up to steal credit info

"NewsScan" <newsscan@newsscan.com>

Wed, 11 Dec 2002 09:54:22 -0700

A Web site called ebayupdates.com, having no relation to the eBay auction site, was created as part of a scam to obtain credit information

fraudulently from eBay customers. The scam was discovered by the private Internet watchdog group SANS Institute Internet Storm Center, and was confirmed by an eBay executive who said: "Some members have reported attempts to gain access to their personal information through e-mail solicitations that are falsely made to appear as having come from eBay. These solicitations will often contain links to Web pages that will request that you sign in and submit information. eBay employees will never ask you for your password." [Reuters/*San Jose Mercury News*, 11 Dec 2002; NewsScan Daily, 11 December 2002
<http://www.siliconvalley.com/mld/siliconvalley/4713932.htm>

✶ Feds raid Ptech looking for al Qaeda link

"Peter G. Neumann" <neumann@csl.sri.com>
Tue, 10 Dec 2002 13:07:17 PST

On 6 Dec 2002, Federal agents raided Ptech in Quincy, Massachusetts, reportedly under suspicion of financial links to Osama bin Laden. Ptech provides unclassified software to many U.S. Government agencies and armed services), and thus there suspicions were raised regarding possible Trojan horses installed in their software. However, on 9 Dec 2002, Justice Department officials said that they do not have any reason to believe any federal systems have been compromised. The search was reportedly done "in

connection with an on-going financial crime investigation," according to a U.S. Attorney, rather than part of any terrorist investigations. [Sources: (1) Feds Raid Boston Area Computer Firm Suspected of Links to Al Qaeda Brian Ross, 6 Dec 2002, courtesy of Monty Solomon http://www.abcnews.go.com/sections/GMA/DailyNews/terror_raid021206.html (2) Justice states Ptech presents no security risk, Wilson P. Dizard III and Patience Wait, *Post Newsweek Tech Media*, 9 Dec 2002, courtesy of Lillie Coney at ACM; severely-PGN-ed]

🔥 Web Surfers: What could they be thinking?

"NewsScan" <newsscan@newsscan.com>

Tue, 10 Dec 2002 08:47:04 -0700

A study by Aaron Schatz has found that the top ten search terms used on Lycos Net this year have been: 1, Dragonball (the Japanese cartoon); 2, Kazaa (the music and video file-swapping service); 3, tattoos (that's right -- tattoos); 4, Britney Spears, the pop singer who, oops, did it again; 5, Morpheus (file-swapping); 6, NFL, the National Football League; 7, IRS; 8, Halloween; 9, Christmas; and 10, Pamela Anderson, the actress and, uh, celebrity icon. Schatz says, "No matter how the news ebbs and flows, people still use the Internet for entertainment." So we see. There just doesn't appear to be that big a demand for information on the origins of the First World War. [*USA Today*, 10 Dec 2002; NewsScan Daily, 10

December 2002]

<http://shorl.com/fovikinustuko>

✶ UK police offer anonymity to cybercrime victims

"Peter G. Neumann" <neumann@csl.sri.com>

Tue, 10 Dec 2002 10:24:15 PST

To overcome the natural reticence companies have against exposing the cases in which they have been victimized by digital attacks, Britain's National Hi-Tech Crime Unit (NHTCU) says it will grant full anonymity to businesses, if they are forthcoming. This is of course not a new concept, but is being tried in hopes it will encourage greater cooperation. [Source: zdnet/Reuters, 9 Dec 2002; PGN-ed, courtesy of Keith Rhodes] <http://zdnet.com.com/2110-1106-976530.html>

✶ Anti-worm "throttling"

Rob Slade <rslade@sprint.ca>

Mon, 9 Dec 2002 12:36:10 -0800

In a number of recent presentations, I have been asked about virus "traps" or "tarpits." The references are to the idea of throttling, and I have finally found the actual paper, rather than the news stories about it:

<http://www.hpl.hp.com/techreports/2002/HPL-2002-172.pdf>

The idea is simple and (within a limited scope) potentially quite effective.

Simply include, in the network stack, programming to limit the number of connections that any computer is making. In particular, limit "new" connections, to machines not normally dealt with. This ensures that normal work, at human generated speeds, proceeds normally, while automated, random connections are restricted.

There are a few caveats to make. The paper refers to viruses, and, of course, what throttling would block are not viruses but classic worms, which make direct connections to other machines. In particular, email viruses might be somewhat restricted, but a Melissa or Loveletter situation would likely be slowed only marginally: connections to the regular mail server would not be "new." Throttling will only be effective against "fast burners": it would definitely help in a situation like the Code Red infestation where a third of a million machines were infected within hours. Slower infectors would be less impeded, and a number of viruses and worms restrict their own spread in order to avoid detection. In addition, a number of viruses now work by replacing the network stack, and therefore this protection would be lost, unless additional protections were layered around the stack. (It would also be fairly simple for viruses or worms to simply start carrying their own network stack.)

rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

<http://victoria.tc.ca/techrev> or <http://sun.soci.niu.edu/>

[~rslade](#)

✶ More on dangers of spelling correctors

Gene Spafford <spaf@cerias.purdue.edu>

Sun, 8 Dec 2002 14:12:39 -0500

So, in one of my many editorial positions, I sent something out for review to several colleagues. One question I asked was "Is this paper significantly different from the same authors' workshop XYZ paper? If not, then we will not publish it again, as a matter of editorial policy."

One of the reviewers returned a review that was negative but insightful. However, it ended with:

"I think that the paper published in XYZ Workshop is a core part of this paper, although the authors did add some new excrement results."

Well, I think that sums up the rest of the reviews I have seen about the paper, but perhaps a bit more candidly than usual! :-)

I asked (politely) if something else had been intended and a transcription error had occurred. I got as a response:

"Very Sorry!! It should be "experiment". It's a typo. MS Outlook corrected it as "excrement" when it checks spelling and I didn't pay attention.... Very embarrassing, but it's all Bill Gates' fault."

Yet another reason I don't use Outlook.....

[Mor(e-)on spelling correctors? PGN]

✶ Your empty mailbox is full

Peter Kaiser <kaiser@acm.org>

Tue, 10 Dec 2002 19:39:33 +0100

Once upon a time I was the customer of a local ISP, Internet Access AG, that had an excellent support line, competent people, and excellent dialup coverage here in Switzerland. They were bought out by a third-tier telephone company that needed an ISP arm quickly. Things were undisturbed: same e-mail address, same people, same location, same quality of service.

Somewhat later the third-tier company was bought out by a second-tier telephone company, call it Sunrays. I could keep the old address. I was still a paying customer, although Sunrays also offers free accounts.

Sunrays has a history of obtuseness about the Internet and Internet service -- for instance they don't seem able to distinguish what should and what needn't be done through secure web pages, they mix languages carelessly (pages are available in German, French, Italian and English), and the FAQs are a bad joke. Long ago I remarked this to a company officer I know socially, and his response was a shrug and a "not my department".

This didn't matter much to me, though. I use their Internet service only

for mail, directly through a POP3 server.

Late last week they began rejecting my incoming mail, and all that was in
in my POP3 mailbox was this message:

Your mailbox is full! It is currently over its allowed capacity.

But except for that message the mailbox was empty.

Here I discovered that even for paying customers their only Internet support other than the FAQs is a premium-priced phone line, another example of not getting it. (I omit a long and familiar kind of tale about how long it took and what I had to do to get anyone to pay attention to the problem.)

Here's what had happened.

On 7 August, with no notice to me, they began filtering spam. The filtered mail is directed to a mail folder named "Spam" which is visible only to users of the browser interface or MS Outlook. I use neither. Between August and late last week they had filed enough mail there to occupy my account's entire storage quota. I was eventually told I had to log on to the Web interface -- my first time using it -- where I was able to see the situation and empty that folder. He tells me they're thinking of sweeping spam folders automatically when they near being over quota, but that's for the future.

After clearing out all the spam -- there seemed to be no false positives,

which is consistent with how much still gets through -- I went to the "personalization" page, where I checked the box for Sunrays to send me their Internet-matters newsletter. But the server wouldn't accept that change unless I also added a whole lot of other information including my birthdate, telephone number, address, and many other things they have no need to know, or already have on file. So no change.

Obviously there's a lot wrong here.

It's clearly a RISK to assume that all their customers are using the mail service through their web interface, where Sunrays may well have posted something about their technique of filtering spam. As a matter of fact, they know perfectly well that some customers are using POP3, because one of their rare useful FAQs is a POP3 how-to for the Eudora mail client.

It's clearly RISKY to send an unclear message when you could perfectly well send an informative one.

It's RISKY to send such messages only when the damage has already been done; for instance, they should send (informative) warning messages long before the user's space is over quota.

And so on. As remarked above, they really don't get it. I'll be shopping for a better service. And perhaps offering them my own services, since I can be bought. But I don't expect them to understand any of this.

✉ Re: Windows 2000 EAL4 Evaluation

Rick Smith <smith@smat.us>

Thu, 05 Dec 2002 23:25:41 -0700

While on one hand I don't believe that EAL4 is an especially strong statement, particularly given the protection profile being used, I think Jonathan Shapiro's comments miss the mark.

Today, EAL4 is the best we're going to see in a large scale commercial product evaluation. The security community barely knows how to do EAL4 in a consistent, cost-effective manner: don't expect to see higher levels except for small-scale things like smart cards.

If EAL4 doesn't provide value to the customers of the evaluated products, then our whole notion of evaluation is flawed (and it just might be).

Regarding EAL7:

>As I mentioned before, EAL levels run from 1 to 7. EAL1 basically means that
>the vendor showed up for the meeting. EAL7 means that key parts of the
>system have been rigorously verified in a mathematical way.

EAL7 isn't the solution, it's just another problem. We're still learning what "key parts" we're supposed to verify, and what it is we might want to prove about them. Windows has huge chunks of behavior that people rely on every day, and only a tiny fraction of those behaviors can be effectively

modeled in a mathematical way. Without a rigorous model you can't do that rigorous proof, and we aren't going to give up word processing simply because we can't prove mathematically that "undo" always works correctly.

Regarding EAL4:

>EAL4 means that the design documents were reviewed using non-challenging
>criteria. This is sort of like having an accounting audit where the auditor
>checks that all of your paperwork is there and your business practice
>standards are appropriate, but never actually checks that any of your
>numbers are correct. An EAL4 evaluation is not required to examine the
>software at all.

While I like the choice of an audit as an analogy, the analogy is wrong.

Having lived through various evaluation activities, I can attest to the fact that you DO have to show that your numbers are correct, even at EAL4, and you have to show it in the manner that most third parties are going to respect: you do a lot of requirements-based testing and you have to show that the testing covers all of your security requirements.

While it is true that the criteria for the design document review might not be especially strict, at least in comparison to doing formal proofs, that part of the process gets very expensive, especially for US-based evaluations. Why? Because you can't use your off-the-shelf design documents: you have to rewrite them to satisfy the evaluators. This is getting better,

but it's still a source of high costs and uncertain schedules.

>An EAL4 rating means that you did a lot of paperwork related to the software
>process, but says absolutely nothing about the quality of the software
>itself. There are no quantifiable measurements made of the software, and
>essentially none of the code is inspected. Buying software with an EAL4
>rating is kind of like buying a home without a home inspection, only more
>risky.

Very wrong. Home inspections are based on external inspections of major components and possibly a few tests like water quality, radon, lead, asbestos, etc. Inspectors rarely disassemble the house to compare the internal structure against the blueprints. And few home inspectors actually try to burn the flameproof drapes, but that's what you'd need to do for EAL4 if your Security Target says your drapes are flameproof.

>Security isn't something that a large group can do well. It is something
>achieved by small groups of experts. Adding more programmers and more
>features makes things worse rather than better. Microsoft has been adding
>features demanded by their customers for a very long time.

I'd argue that the problem isn't so much the size of the team as it is the discipline applied to managing the architecture. Without a strong security architecture in place, it doesn't matter how many people work on the system -- it'll still be Swiss cheese.

>It is possible to do much better. EROS, a research operating

system that we
>are working on here in the Systems Research Laboratory at Johns
Hopkins
>University, should eventually achieve an EAL7 evaluation
rating, and is
>expected to provide total defense against viruses and malicious
code.

I think such systems will provide a strong basis for special-
purpose
devices, but I doubt they'll replace desktop systems, which
become a lot
like one's office: a mishmash of what you need to get through
the day and
hopefully be productive. If people have EROS on their desktops,
it'll stay
virus proof right up until they start installing all those virus-
enabled
e-mail products and word processors they love so much. This is a
variant of
the "GOVNET" problem - GOVNET was a boondoggle because it
focused on ISO
layers 4 and below, ignoring the growing problem of virus-laced
e-mail and
shared Word documents.

Rick Smith (smith@smat.us) Oxford International, Scottsdale, AZ

[The most fundamental problem with the evaluation process is
that the

evaluation is done against criteria evaluation profiles that
are

established by the organization seeking evaluation. The MS
EAL4 is rather

lame primarily because the evaluation profiles are not very
comprehensive.

However, as Rebecca Mercuri's thesis shows in her casting of
electronic

voting systems into the Common Criteria framework, EVEN IF THE
EVALUATION

CRITERIA ARE VERY ELABORATE, THEY ARE STILL INHERENTLY
INCOMPLETE and

significant security vulnerabilities can still remain. PGN]

REVIEW: "VPNs: A Beginner's Guide", John Mairs

Rob Slade <rslade@sprint.ca>

Fri, 22 Nov 2002 07:42:10 -0800

BKVPNABG.RVW 20020928

"VPNs: A Beginner's Guide", John Mairs, 2002, 0-07-219181-3, U
\$39.99

%A John Mairs

%C 300 Water Street, Whitby, Ontario L1N 9B6

%D 2002

%G 0-07-219181-3

%I McGraw-Hill Ryerson/Osborne

%O U\$39.99 +1-800-565-5758 +1-905-430-5134 fax: 905-430-5020

%P 584 p.

%T "VPNs: A Beginner's Guide"

Part one deals with networks and security. The material is not bad;

in fact, it is very good; but it is, possibly, too much information on

topics which are not, really, relevant to virtual private networks

(VPNs). On the other hand, anyone who is a rank beginner to networking as well will certainly have a thorough introduction.

Chapter one covers layering architecture and the OSI (Open Systems

Interconnection) model, and the text on encapsulation is definitely

relevant to VPNs. Network architecture, in chapter two, concentrates

on topology and the physical layer. There is a detailed reference to

the lower layers of the TCP/IP protocol stack in chapter three.

Chapter four's explanation of the basics of security is good, absent

some material on threats and parts of risk analysis, but the use of non-standard language may be confusing. Threats and attack methods, in chapter five, is weak: the text lists a variety of network protocol exploits, concentrating on spoofing, and doesn't really bring out the concepts. The explanations of intrusion detection systems and firewalls, in chapters six and seven respectively, are good overviews.

Part two is supposed to provide the fundamentals of VPNs themselves, but, rather oddly, does a much poorer job on this central idea than on the previous and following content. Chapter eight is on VPN basics, and nine is on VPN architecture.

Part three covers VPN protocols. Chapter ten introduces the tunneling protocols of GRE (Generic Routing Encapsulation) and PPTP (Point-to-Point Tunneling Protocol). L2F (Layer 2 Forwarding) and L2TP (Layer 2 Tunneling Protocol), plus a little bit of IPSec, are reviewed in chapter eleven, although it is not always clear what functions are supported.

Part four looks at secure communications. The material on cryptography, in chapter twelve, is not very good: polyalphabetic ciphers are **not** examples of transposition, there is some use of non-standard terminology, the text is simplistic in many areas, and the discussion of key management with asymmetric systems is quite weak. There are similarly feeble explanations and minor errors with respect to cryptographic algorithms in chapter thirteen. The discussion of

certificates, in chapter fourteen, is more reasonable, although the section on PKI (Public Key Infrastructure) is a bit terse. Chapter fifteen, on authentication, reprises earlier content on identification and authentication (chapter four), PAP (Password Authentication Protocol, chapter ten), CHAP (Challenge Handshake Authentication Protocol, chapter eleven), but adds discussion of RADIUS, TACACS, and Kerberos, at varying levels of detail.

Part five delves into the details of IPSec. Chapter sixteen outlines the components of IPSec, although it is somewhat disjointed with repeated returns to the topics of security associations and the different operating modes. Key management, in chapter seventeen, introduces ISAKMP (Internet Security Association and Key Management Protocol) and IKE (Internet Key Exchange), but does not do so in the detail with which other protocols have been discussed, and does not address the weaknesses of the systems. For some reason the details, and some other key management and exchange protocols, are in chapter eighteen (but still limited analysis). Chapter nineteen does have good deliberations on IPSec architecture and implementation.

Part six deals with MPLS (Multi-Protocol Label Switching). Chapter twenty talks about quality of service, and related technologies. A few topics associated with traffic engineering are discussed in chapter twenty one. MPLS is proposed as the answer to quality of service and traffic engineering issues in chapter twenty two. Chapter twenty three outlines some of the components of MPLS and finally explains what MPLS has to do with VPNs, although not in much detail.

With some caveats about certain sections of the book, I can recommend this both as a reference to a number of VPN technologies, and to some security related issues with TCP/IP.

copyright Robert M. Slade, 2002 BKVPNABG.RVW 20020928
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

🔥 REVIEW: "IPSec: Securing VPNs", Carlton Davis

Rob Slade <rslade@sprint.ca>
Mon, 2 Dec 2002 08:00:16 -0800

BKIPSECS.RVW 20021001

"IPSec: Securing VPNs", Carlton Davis, 2001, 0-07-212757-0,
U\$49.99/C\$79.95/UK#36.99
%A Carlton Davis carlton@cs.mcgill.ca
%C 300 Water Street, Whitby, Ontario L1N 9B6
%D 2001
%G 0-07-212757-0
%I McGraw-Hill Ryerson/Osborne
%O U\$49.99/C\$79.95/UK#36.99 800-565-5758 fax: 905-430-5020
%O [http://www.amazon.com/exec/obidos/ASIN/0072127570/
robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/0072127570/robsladesinterne)
%P 404 p.
%T "IPSec: Securing VPNs"

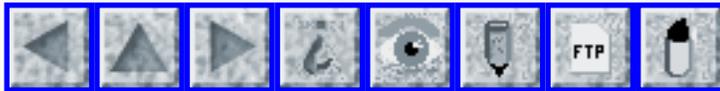
Chapter one is an overview of TCP/IP. The material is generally good, but does demonstrate a possible weakness of the book: we are provided with way too much information about a number of areas that are not relevant to IPSec. A similar overabundance of detail (and math) describes symmetric cryptography, in chapter two. Oddly, given

the level of particulars in other areas, there is no analysis of the weakness of double DES (Data Encryption Standard). Operational specifics of the various AES (Advanced Encryption Standard) candidates are also included. The mathematical basis of asymmetric cryptography, in chapter three, is not explained as well as symmetric is. In dealing with hashes and message authentication codes, chapter four has lots of math and almost no other discussion. Chapter five provides extensive details about X.509 attribute fields, for digital certificates, and also has a bit of material on PGP (Pretty Good Privacy) and key recovery. The fields of LDAP (Lightweight Directory Access Protocol) are outlined in chapter six.

Chapter seven finally talks, very briefly, about IPsec architecture, repeating (from chapter one) the specifics of the IP header, and mentioning some of the components of IPsec. Chapters eight, nine, and ten concentrate on the header structure of AH (Authentication Header), ESP (Encapsulating Security Payload), and ISAKMP (Internet Security Association Key Management Protocol) packets, albeit chapter ten also covers a bit of the handshaking process. There is very little discussion of strengths and weaknesses. There are lots of details related to IKE (Internet Key Exchange) in chapter eleven, but surprisingly little information about what it does or how it works. The header structure and options for the compression function, IPComp, are given in chapter twelve. Chapter thirteen is supposed to talk about implementation, but has a fairly generic example of a VPN and some screen shots from a commercial product.

Overall, the book contains lots of technical details, but very little in the way of explanation, discussion, or analysis. You would probably learn just as much about IPSec by reading the RFCs themselves.

copyright Robert M. Slade, 2002 BKIPSECS.RVW 20021001
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

[ACM](#) Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 43

Monday 16 December 2002

Contents

- [Bad circuit crashed \\$150 million jet at Woomera](#)
[George Michaelson](#)
- [Senate closes accidental anonymizer](#)
[Dave Stringer-Calvert](#)
- [More on identity thieves strike eBay, whose policies make it worse](#)
[Elana](#)
- [Australian ruling is raising worries](#)
[Monty Solomon](#)
- [Moore's Law hits a leak](#)
[NewsScan](#)
- [Paypal scam?](#)
[Dawn Cohen](#)
- [Internet spam mogul can't take what he dishes out](#)
[Purkasz](#)
- [Tower reports customer information "leak"](#)
[B Crook](#)
- [Perils in switching to Yahoo](#)
[David Lazarus via Monty Solomon](#)
- [Community security education contacts](#)
[Rob Slade](#)

- [U.S. Army Research Office Calls For Odortype Detection Proposals](#)
[PGN](#)
 - [Re: Anti-worm "throttling"](#)
[Jeremy Epstein](#)
 - [The risks of RISKS](#)
[Donald A. Norman](#)
 - [REVIEW: "The Art of Deception", Kevin D. Mitnick/William L. Simon](#)
[Rob Slade](#)
 - [REVIEW: "Secured Computing", Carl F. Endorf](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ **Bad circuit crashed \$150 million jet at Woomera**

George Michaelson <ggm@apnic.net>
Thu, 12 Dec 2002 09:39:15 +1000 (EST)

A computer glitch has been blamed for July's disastrous launch of a Japanese supersonic jet model at South Australia's Woomera rocket range. Japan's National Aerospace Laboratory says a design change caused the \$150 million scale model's computer system to short-circuit. Flight director Kimio Sakata says the autopilot then reset itself and caused the jet and rocket booster to separate during take-off.

<http://www.abc.net.au/news/justin/nat/newsnat-12dec2002-22.htm>

Hmm. sounds like bad design *processes* as much as a computer glitch...]

✶ **Senate closes accidental anonymizer**

Dave Stringer-Calvert <dave_sc@csl.sri.com>

Wed, 11 Dec 2002 15:39:27 -0800

Never let it be said that the United States Senate has done nothing for Internet privacy. Network administrators for the U.S. government site www.senate.gov shut down an open proxy server over the weekend that for months had turned the site into a free Web anonymizer that could have allowed savvy surfers to launder their Internet connections so that efforts to trace them would lead to Capitol Hill. A proxy server is normally a dedicated machine that sits between a private network and the outside world, passing internal users' Web requests out to the Internet.

<http://online.securityfocus.com/news/1780>

✶ Identity thieves strike eBay, whose policies make it worse

Elana Who? <falcospav@excite.com>

13 Dec 2002 06:05:23 -0800

We recently had an article in comp.risks titled "Identity thieves strike eBay". Below, author Spider Robinson reports how he was victimized, plus details on the not-very-good way that eBay handled it, all which made the situation worse. Mr. Robinson has been robbed by almost a thousand dollars because of it.

<http://www.theglobeandmail.com/servlet/ArticleNews/PEstory/>

[TGAM/20021211/COSPIDER/Columnists/columnists/
columnistsNational_temp/1/1/6/](http://www.theglobeandmail.com/servlet/ArticleNews/PEstory/TGAM/20021211/COSPIDER/Columnists/columnists/columnistsNational_temp/1/1/6/)

[http://www.theglobeandmail.com/servlet/ArticleNews/PEstory/TGAM/
20021211/COSPIDER/Columnists/columnists/
columnistsNational_temp/1/1/6/](http://www.theglobeandmail.com/servlet/ArticleNews/PEstory/TGAM/20021211/COSPIDER/Columnists/columnists/columnistsNational_temp/1/1/6/)

✶ Australian ruling is raising worries

Monty Solomon <monty@roscom.com>

Mon, 16 Dec 2002 09:01:00 -0500

A number of concerned First Amendment advocates say a landmark libel decision by the Australian High Court may have the effect of erecting a fence on the borderless information frontier opened up by Internet technology. The 10 Dec 2002 ruling concluded that an Australian businessman, Joseph Gutnick, could sue Dow Jones for defamation in Australia based on a Barron's magazine story that emanated from the company's computer servers in New Jersey. Although, as attorney Harvey Silverglate explains, defamation cases have traditionally been brought "in the jurisdiction where the speech is uttered or published or where you targeted it," the ruling effectively expanded that jurisdiction in the online world to where a story can be downloaded. The case involves a "United States media publication which is really focused on United States markets and United States investors" and "a journalist who operated completely out of the United States," says Stuart Karle, a Dow Jones associate general

counsel. ' 'This dramatically changes how you can communicate within this country. ' '

[Source: Mark Jurkowitz, *The Boston Globe*, 16 Dec 2002]

http://www.boston.com/dailyglobe2/350/business/Australian_ruling_is_raising_worries+.shtml

[All sorts of implications. PGN]

✶ Moore's Law hits a leak

"NewsScan" <newsscan@newsscan.com>

Thu, 12 Dec 2002 09:20:13 -0700

Intel chairman Andy Grove warned participants at the International Electron Devices Meeting this week that electrical current leakage from inactive processors poses a major challenge to the continued viability of Moore's Law (which predicts the doubling of transistor densities every couple of years). "Current is becoming a major factor and a limiter on how complex we can build chips," said Grove, who added that his company's engineers "just can't get rid of power leakage." As chips become more powerful, leakage rates increase, and while the industry is accustomed to low-level leakage rates, high-end chips made up of a billion transistors may leak between 60 and 70 Watts of power, causing problems with cooling. Grove also warned that the trend of migrating chip manufacturing to Asian plants could shift the balance of power eastward. "It is easy to project that the independence

becomes more one-sided, with an adverse impact on our educational system because so much of the university funding comes from industry. There is a spiral there in the wrong direction." [Computerwire/The Inquirer 11 Dec 2002; NewsScan Daily, 12 Dec 2002]
<http://www.theinquirer.net/?article=6677>

Copyright 2002. NewsScan Daily (R) is a publication of NewsScan.com Inc.
Reproduced in RISKS with permission.

✶ **Paypal scam?**

"Dawn Cohen" <COHEND@wyeth.com>
Fri, 13 Dec 2002 17:13:31 -0500

I received an e-mail with the subject:

"Paypal Alert: Please Update your current Billing Information"

In that I don't have a paypal account, I was a little curious, and decided to investigate. When I looked at the message, I saw what appears to be a scam:

"Unfortunately today we have had some trouble with one of our computer systems. While the trouble appears to be minor, we are not taking the necessary precautions. We have decided to take the affected system offline and replace it with a new system. Unfortunately this has caused us to lose member data and information. Please follow the link=link below and log into your account to re-enter your information to be assured

none of your

prior information has been lost. Please Note: Account balances have not been affected."

Then there is a link "Click Here To Begin the Account Process", with a link that goes (upon examination of the source HTML) to an IP address at some Autobahn Access Corporation.

The message was very cleverly constructed, to use Paypal images (based on their own urls)

```
<A href=3D"https://www.paypal.com/" target=3D_blank><IMG  
height=3D35  
alt=3DPayPal src=3D"http://www.paypal.com/images/email_logo.  
gif" width=3D25  
5 border=3D0></A>
```

And it had a reply-to address of customerservice@paypal.com. (They were careful to say in the message, though, "Please do not reply to this e-mail. Mail sent to this address cannot be answered.")

Internet spam mogul can't take what he dishes out

<PURKASZ@aol.com>

Thu, 12 Dec 2002 20:43:10 -0500

West Bloomfield (Michigan) bulk e-mailer Alan Ralsky, who just may be the world's biggest sender of Internet spam, is getting a taste of his own medicine. Ever since I wrote a story on him a couple of weeks ago (www.freep.com/money/tech/mwend22_20021122.htm), he says he's been inundated with ads, catalogs and brochures delivered by the U.S. Postal Service to his

brand-new \$740,000 home. It's all the result of a well-organized campaign by the anti-spam community, and Ralsky doesn't find it funny. ... [Source: Mike Wendland, *Detroit Free Press*, 6 Dec 2002]

⚡ Tower reports customer information "leak"

<bcrook0926@rogers.com>

Thu, 12 Dec 2002 12:52:49 -0500

Tower Records, a well known chain of record shops that does business in the US and the UK, recently suffered an embarrassing information leak due to amateurish Web programming. A Windows "Active Server Page" script, which allowed customers to check the status of their orders by entering their order numbers, was written so that it required no other identification from the user than the order numbers themselves -- which were assigned in sequence. Simply modifying a URL to contain an order number one greater or one less than that assigned to your own order would show you another customer's information. E-mail addresses, street addresses, phone numbers, and order information dating back to 1996 were exposed. The chain reports that the hole was finally closed this week.

<http://www.extremetech.com/article2/0,3973,760739,00.asp>

⚡ Perils in switching to Yahoo (David Lazarus)

Monty Solomon <monty@roscom.com>

Fri, 13 Dec 2002 22:15:48 -0500

David Lazarus, *San Francisco Chronicle*, 13 Dec 2002

Pacific Bell may be taking on a new name, but it's still up to the same old tricks. The company's customers were outraged when I wrote how Pac Bell, which now wants to be known by the moniker of its corporate parent, SBC, slipped an insert into recent bills advising that personal information will be shared with business partners unless the customer says otherwise. ... That's not the half of it. For some services, Yahoo says it will request Pac Bell customers' Social Security number "and information about your assets." The online company says it will track DSL subscribers' Internet browsing and share personal information with "trusted partners." Such info will be used in part "to customize the advertising and content you see." "Once you create an SBC Yahoo account and sign in to our services, you are not anonymous to us," Yahoo warns in surprisingly stark language. ...

<http://sfgate.com/cgi-bin/article.cgi?f=/c/a/2002/12/13/BU191399.DTL>

Community security education contacts

Rob Slade <rslade@sprint.ca>

Tue, 10 Dec 2002 16:22:55 -0800

Many of us have known for years that education and heightened awareness are vital to improving the general information security situation. It's been rather frustrating to try and promote the idea. However, at long last there seems to be a groundswell of both interest in the topic, and work towards producing seminars and training.

As a step in getting some cooperation going in terms of the production of security awareness seminars, I have started a mailing list and a Web page of contacts. The mailing list is comseced@yahoogroups.com: if you want to join send e-mail to comseced-subscribe@yahoogroups.com. The Web page is at <http://victoria.tc.ca/techrev/comseced.htm> or <http://sun.soci.niu.edu/~rslade/comseced.htm>.

If you have curricula, materials, or ideas that you would be willing to share, please drop me a line or join the group.

rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com
<http://victoria.tc.ca/techrev> or <http://sun.soci.niu.edu/~rslade>

U.S. Army Research Office calls for odortype detection proposals

"Peter G. Neumann" <neumann@csl.sri.com>
Mon, 16 Dec 2002 9:57:05 PST

<<http://www.aro.army.mil/research/index.htm>>

The U.S. Army Research Office (ARO) is soliciting proposals to

determine whether genetically-determined odortypes may be used to identify specific individuals. The proposal also calls for development of the science and enabling technology to detect and identify specific individuals by such odortypes. The Odortype Detection Program will leverage research that has demonstrated that the same set of genes that code for internal immune system self/non-self recognition in mice -- the Major Histocompatibility Complex (MHC) -- also code for individual odortype. Total funding for the research and development effort may be up to \$3.2 million in 2003.
<http://www.biometritech.com/enews/121602c.htm>

[De-scent into the pits? PGN]

✶ Re: Anti-worm "throttling"

<jeremy.epstein@cox.net>
Thu, 12 Dec 2002 23:45:25 -0500

The HP paper you're referring to ("Throttling Viruses: Restricting propagation to defeat malicious mobile code" by Matthew Williamson, Hewlett-Packard Labs) was presented this week at the 18th Annual Computer Security Applications Conference, and won the best paper award. Along with Paul Karger's Multics retrospective (discussed in previous issues of RISKS), it's made this year's ACSAC particularly interesting.

⚡ The risks of RISKS

"Donald A. Norman" <don@jnd.org>

Mon, 16 Dec 2002 10:03:49 -0600

The RISK of RISKS:

I've become paranoid over the past year, but legitimately. And it is wrecking my life.

Because I was involved in a National Academies study of anti-terrorism, I examined how people defeated security systems. The security community -- with some notable exceptions -- seems to think this is a technological problem: put in enough technology and the system is secure. I have always thought just the opposite: this is a social problem. Indeed, my belief is that "The more secure you make the system from a technological point of view, the less secure you are apt to have made it in reality." Why? Because the technology gets in the way of work, and so the most dedicated workers will defeat the system in order that they can get their work done. My studies of the cracker community and discussions with professional "red team" members simply reinforces the view.

We are social beings: we work well in small, cooperative groups. Part of the benefits of our society is that we all help one another. We trust one another. The people who would deceive us understand this and manipulate it.

Well, the social engineer takes advantage of all of this. I've just finished reading the book by Mitnick and Simon. I recommend it to everyone: it is scary. It tells how a few simple sounding (but very sophisticated) phone calls can get the sophisticated con artist almost anything. It gives very convincing examples.

Mitnick, K. D., & Simon, W. L. (2002). The art of deception: controlling the human element of security. Indianapolis: Wiley.

So now I am on guard. And guess what, I immediately spot spoofs. I get an e-mail stating that I have just signed up with American Express for bill-paying, so I should log on to this URL and set up my account. Except that I didn't recall signing up, and the URL is not associated with American Express : it is "thevalidnetwork.com" . Sounded like a spoof to me. I call up American Express. They deny all knowledge of the site, but they also refuse to accept my complaint. "Not my department," said the woman, as she gave me a different phone number to call and hung up on me. The man at the other phone number also confirmed that this was not a valid American Express site, and he wanted to report it, but it wasn't his responsibility either -- the phone number he asked me to use was for the woman who refused to take it. He tried -- he was turned down too.

So American Express claims this is not their site, but refuses to let me file a complaint.

Then yesterday, I get a letter inviting me to a conference. Would I send my

address and phone number, and also the phone numbers of anyone else I thought should be invited. The person said he had gotten my name from X, and said the conference was run by Consumers Reports. Well, the website he listed gave no hint of why I should trust this person -- he claimed to be a contractor. I checked with X, who said, no, he couldn't vouch for the person. The letter said time was of the essence, but it came in over the weekend, so I couldn't call Consumer Reports to check.

Both letters were perfect examples of Mitnick's illustrations of how to con people. They look legitimate, but if you examine them closely, the URLs are wrong, and although legitimate names are given, this is an emergency and the answer must be given now, after hours, when those legitimate-sounding names can't be checked.

I now have discovered that both e-mails were legitimate. My financial advisor had signed me up for the bill payment scheme (he says we asked him to). The site was subcontracted by American Express to do this, but obviously, their phone support people don't know this. As for the invitation, the person at Consumer Reports vouched for it.

But what a life we have to lead: we can easily be conned by legitimate looking requests. And we might refuse to honor legitimate requests that could also be frauds. Or, even if we accept them, we waste a lot of time checking them out -- a lot of our time and that of the people we have to bother to find out if it is real. And, along the way, I also

discovered that even if we are recipients of a real fraud, it is very difficult to tell anyone. An amazing number of websites lack any contact information, any way of reporting problem. And even if you do report a problem, it is answered bizarrely. I just reported over a website to Mindspring that their server seemed to be down. In reply I was told how to check the modem settings under Windows 98. That wasn't my complaint, I don't use a dial-up modem, and I don't run Windows 98. When I complained that the response was not relevant, I got instructions to check the wiring of my modem.

So consider the RISKS of RISKS. We waste time every day deleting spam and backing up our systems. We waste time every week updating our virus controls and rescanning our computer systems. We no longer can trust the people we interact with, for social engineers take advantage of all that we have come to trust. We are searched at work and when traveling. We have to watch what we say in public because it might be misinterpreted. And there is nobody to complain to.

Trust is rapidly leaving our society, and we all are worse off as a result.

Don Norman, Prof. Computer Science, Northwestern University

<http://www.jnd.org>

and Nielsen Norman Group

<http://www.nngroup.com>

norman@nngroup.com

[See Rob Slade's following item. PGN]

REVIEW: "The Art of Deception", Kevin D. Mitnick/William L. Simon

Rob Slade <rslade@sprint.ca>

Thu, 12 Dec 2002 08:00:51 -0800

BKARTDCP.RVW 20021028

"The Art of Deception", Kevin D. Mitnick/William L. Simon, 2002, 0-471-23712-4, U\$27.50/C\$39.95/UK#19.95

%A Kevin D. Mitnick

%A William L. Simon

%C 5353 Dundas Street West, 4th Floor, Etobicoke, ON M9B 6H8

%D 2002

%G 0-471-23712-4

%I John Wiley & Sons, Inc.

%O U\$27.50/C\$39.95/UK#19.95 416-236-4433 fax: 416-236-4448

%O <http://www.amazon.com/exec/obidos/ASIN/0471237124/>

[robsladesinterne](#)

%P 352 p.

%T "The Art of Deception: Controlling the Human Element of Security"

Those in the security field know that Kevin Mitnick does not deserve the reputation he has gained as some kind of technical genius. His gift was skill as a social engineer. Stripped of the five dollar words, this means that he was a plain, old con man, cheat, or fraud. In other words, this is a book about how to fool people. Theoretically, the determined reader should be able to use the book to keep from being conned.

In the preface, Mitnick would have us believe that, although he admits to being a fraud and deceiver, he was never a grifter. He never harmed anybody, never obtained a material benefit, and was just curious

to see if he could ride the buses for free (at the expense of the transit system) or make calls for free (at the expense of an MCI customer). (The willing moral blindness of these assertions is possibly the most instructive part of the book: it is truly representative of large portions of the blackhat community.) He would have us believe that he is a "changed person": one of the most sought-after computer security experts world-wide, and the world's most famous hacker. Oh, and just in case the authorities are inclined to think that this book runs counter to the injunction that he not profit from the stories of his criminal exploits, the tales are all completely fictional. Trust him.

Part one is entitled "Behind the Scenes." Chapter one states that people are security's weakest link. This is a truism well known in the field, but the first account is really about insider fraud, while the remainder are generic fear-mongering.

Part two describes the art of the attacker. (At great length.) Chapter two depicts escalation or enumeration through social engineering, and points out that sometimes innocuous information isn't. There is a section on "preventing the con" at the end of each chapter: in this case we are told not to give out information, but not provided with any advice about authenticating callers. Similarly, chapter three says that sometimes attackers just ask for access or information and says to verify callers, but

doesn't say how. Chapter four tells you to distrust everyone-- which would probably be more damaging to society than social engineering. (Interestingly, yesterday a report came out about studies of "freeloading" in the animal kingdom, which notes that communities with too many non-contributing members tend not to survive. By extension, only societies with an overwhelming majority of trustworthy members exist for any length of time.) The prevention bit tells companies not to have people give credit card information over the phone, but stresses teaching employees about cons rather than policies. At about this point the text, which is very repetitious, throws in some minor technical details. This is enough to remind the professional that the book is designed for the naive user, with extremely lightweight analysis, and implications that would not be useful. There is more repetitive redundancy in chapter six, on the way to some useful information about fraudulent e-mail and really lousy data about viruses and malware, in chapter seven. Chapters eight and nine are simply more of the same stories, which start to get very tedious.

Part three is apparently supposed to help us detect intruders. Chapter ten has a little useful advice about having termination procedures. The major points in chapter eleven seem to be about all the people who have been mean to our poor Kevin. Then it is back to the, by now extremely tiresome, con jobs for another three chapters.

We are intended to believe that part four will help us protect ourselves and

our companies against social engineering. Chapter fifteen is an attempt to convince us that the book should be purchased for all employees. (Nice try, Kev.) There is an arbitrary, and oddly both generic and overly detailed, suggested security policy, in chapter sixteen.

So. Security professionals already know about social engineering. It is unlikely in the extreme that even the most head down, don't-talk-to-the-users, socially maladept firewall administrator will learn very much from this book. But, of course, this is not a trade paperback. This is a hardback aimed at the mass market: the non-professionals. Will they learn anything from it? Well, it might be useful for teaching new tricks to those who like to con people (although fraudsters will likely be disappointed at the number of times it is assumed that they know how to reprogram DMS-100 switches: don't try this at home). The prevention sections, as noted, are big on "don't" and short on "how not to."

Well, but the book can still be a fascinating read, can't it? Sure. If you're the type of person who finds humour in watching someone fall on his or her face. Over and over again ...

copyright Robert M. Slade, 2002 BKARTDCP.RVW 20021028
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

<http://victoria.tc.ca/techrev/~rslade> or <http://sun.soci.niu.edu/~rslade>

[See Don Norman's previous item. PGN]

REVIEW: "Secured Computing", Carl F. Endorf

Rob Slade <rslade@sprint.ca>

Wed, 11 Dec 2002 08:12:25 -0800

BKSCDCMP.RVW 20020905

"Secured Computing", Carl F. Endorf, 2002, 1-55212-889-X,
U\$44.95/C\$64.00

%A Carl F. Endorf etresearch@hotmail.com

%C Suite 6E, 2333 Government Street, Victoria, BC V8T 4P4

%D 2002

%G 1-55212-889-X

%I Trafford Publishing

%O U\$44.95/C\$64.00 888-232-4444 FAX 250-383-6804

sales@trafford.Com

%O [http://www.amazon.com/exec/obidos/ASIN/155212889X/
robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/155212889X/robsladesinterne)

%P 538 p.

%T "Secured Computing: CISSP Study Guide, Second Edition"

Like Mandy Andress' book (cf. BKCISPEC.RVW), this concentrates on terminology, rather than the concepts that the CISSP exam actually tests

for. Like Krutz and Vines' book (cf. BKCISPPG.RVW), this obviously and

slavishly follows the (ISC)² syllabus. Unlike Shon Harris' book (cf. BKCISPA1.RVW), it doesn't provide much added value or explanation.

It does offer a money back guarantee. If, within six months of buying the

book, you take the CISSP exam twice (at U\$450 a pop) and fail both times,

you get the price of the book back. Less shipping and handling. (Also, you

might need to be careful when ordering the book. The ISBN is identical for

both the first and second editions.)

Some of the errors in the first edition of the book have been corrected, but a few remain, such as the addition of a "strong star" property to the Bell-LaPadula security model.

Since the work concentrates on jargon, there are glaring gaps in the coverage. For example, the Law, Investigation, and Ethics domain has almost nothing to say about incident response, investigation, preservation of evidence, computer forensics, or interviewing.

Added to the book in this second edition is a practice CISSP exam. Although the structure of the questions appears to be similar to those you would see on a real exam, the answers, oddly enough, rely on nonstandard terminology.

Approximately one third of the total material in the second edition is a reprint of the "Standard of Good Practice" document available from the Information Security Forum (www.securityforum.org). While there is nothing wrong with the document, and it could be a useful aid to the practitioner, it isn't much of a help in studying for the CISSP.

While this book might provide some assistance in exam prep, it is probably not a sufficient guide by itself.

copyright Robert M. Slade, 2002 BKSCDCMP.RVW 20020905
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

<http://victoria.tc.ca/techrev/~rslade> or <http://sun.soci.niu.edu/~rslade>



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

[ACM](#) Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 44

Sunday 29 December 2002

Contents

- [Accidental alert spooks Vermont Yankee neighbors](#)
[Robin Wheeler](#)
- [Pioneer 10 still alive, 30 years later](#)
[PGN](#)
- [More UK air-traffic woes](#)
[Ursula Martin](#)
- [Russian firm cleared in U.S. copyright case](#)
[NewsScan](#)
- [DEA data thief sentenced to 27 months](#)
[PGN](#)
- [Computer programmer faces U.S. fraud charge in virus attack](#)
[Monty Solomon](#)
- [O Big Brother, where art thou? -- everywhere](#)
[NewsScan](#)
- [The Total Information Awareness program is a RISK!](#)
[Edward G. Nilges](#)
- [Old mechanical voting machines also break, but have audit trails](#)
[Danny Burstein](#)
- [Electronic vote machines open to tampering - report](#)
[Derek Harnett](#)

- [Is a cleared check really like money in the bank?](#)
[Sidney Markowitz](#)
 - [Baffling ATM behavior](#)
[Bill Bumgarner](#)
 - [Re: Crackers steal 52,000 university passwords](#)
[Harald Hanche-Olsen](#)
 - [Why you should read Mitnick's book: The risks of seeing the trees](#)
[Don Norman](#)
 - [Surgical tool left in woman's stomach for 4 months](#)
[Keith Rhodes](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ **Accidental alert spooks Vermont Yankee neighbors**

Robin Wheeler <rwheeler@iso-ne.com>

Fri, 27 Dec 2002 10:17:31 -0500

Christmas Day was rough on people in the Northeastern U.S., with snow and nasty weather conditions. One very tired National Weather Service forecaster had worked 24 hours straight, into the following day, because relief could not make it to the Albany NY work site, with up to three feet of snow on the ground. He accidentally clicked on an icon that triggered a high-alert general site emergency to neighbors of the Vermont Yankee nuclear power station, just one level below the evacuation order. That alert went via special tone-alert radios only to people who cannot hear the urban-centered emergency sirens. The alert was canceled shortly thereafter, after the VT Emergency Management Office checked with the power plant. There is a five-minute delay on such alerts going out to the general radio

audiences, so this particular alert never made it more widely than the special alert system. Reportedly, the software will be modified to make this type of erroneous message less likely. [Source: Susan Smallheer, *Rutland Herald* (Vermont), 27 Dec 2002; susan.smallheer@rutlandherald.com; PGN-ed] <http://timesargus.nybor.com/Story/58206.html>;

✶ Pioneer 10 still alive, 30 years later

Peter Neumann <neumann@CSL.sri.com>
Wed, 18 Dec 2002 20:15:39 -0800 (PST)

"A distant Pioneer whispers to Earth": Like the Energizer Bunny, Pioneer 10 is still going after 30 years -- sort of. Silent since March 2002, now 7.5 billion miles away, or 11 hours at the speed of light, faint signals were received but could not be locked on, and no scientific information could be obtained.

<http://www.cnn.com/2002/TECH/space/12/18/pioneer.contact/index.html>

[or <http://reuters.com/newsArticle.jhtml?type=topNews&storyID=1921184> ?]

[typo corrected in archive copy, alternative URL suggested as well. PGN]

✶ More UK air-traffic woes

Ursula Martin <um@dcs.st-and.ac.uk>

Thu, 19 Dec 2002 08:39:17 GMT

The UK National Air Traffic Control Centre at Swanwick ([RISKS-21.98](#), [22.02,03,09,12,13](#)) is still having ``potentially catastrophic'' problems, including erratic communications breakdowns between controllers and pilots, unclear screen images, etc.

http://news.bbc.co.uk/2/hi/uk_news/2589247.stm

✶ Russian firm cleared in U.S. copyright case

"NewsScan" <newsscan@newsscan.com>

Wed, 18 Dec 2002 09:00:59 -0700

ElcomSoft Co. Ltd., based in Moscow, has been found *not guilty* of criminal charges that it violated the 1998 U.S. Digital Millennium Copyright Act by selling a software program designed to circumvent the digital locks used to enforce copyright protections on Adobe Systems e-book software. The two-week trial was the first criminal prosecution under the controversial DCMA, which prohibits the sale of technology that can be used to break the code that "locks" digitally formatted movies, music and other software. The case hinged on whether ElcomSoft had "willfully" violated U.S. law, an intent the defendants denied. "They never intended to violate the law," said defense attorney Joseph Burton. ElcomSoft president Alexander Katalov

pointed out that the program was legal in Russia and was not meant to be used for electronic books that had not been legally purchased. He said he didn't know that the software was illegal under U.S. law.

[Reuters, 17 Dec

2002; NewsScan Daily, 18 December 2002]

<http://shorl.com/degreryliprujy>

✶ DEA data thief sentenced to 27 months

Peter Neumann <Neumann@CSL.sri.com>

Wed, 18 Dec 2002 09:19:01 -0500

Emilio Calatayud, who worked for the U.S. Drug Enforcement Administration (DEA) for 14 years, has now been sentenced to 27 months in prison and a \$5,000 fine for selling information on claimants in more than 1000 workers' compensation cases to Triple Check Investigative Services. He used his authorized access to the FBI's National Crime Information Center (NCIC), the California Law Enforcement Telecommunications System (CLETS), and the DEA Narcotics and Dangerous Drug Information System (NADDIS). He was paid at least \$22,500 from 1993 to 1999 for these extracurricular services. On the first day of his trial in February 2002, he fled to Mexico, but was later caught. [Source: Kevin Poulsen, SecurityFocus Online, 18 Dec 2002; klp@securityfocus.com; <http://www.securityfocus.com/>; PGN-ed; Courtesy of Richard M. Smith <http://www.theregister.co.uk/content/55/28621.html>]

⚡ Computer programmer faces U.S. fraud charge in virus attack

Monty Solomon <monty@roscom.com>

Wed, 18 Dec 2002 22:34:20 -0500

A former UBS PaineWebber computer expert was indicted on federal charges of trying to manipulate the stock price of the brokerage's parent company last spring by disseminating a computer virus among over 1,000 systems used by PW brokers. He had reportedly been hoping to gain from the resulting stock price drop. [Source: article by Robert Hanley, *The New York Times*, 18 Dec 2002; PGN-ed]

<http://www.nytimes.com/2002/12/18/technology/18SABO.html>

⚡ O Big Brother, where art thou? -- everywhere

"NewsScan" <newsscan@newsscan.com>

Mon, 23 Dec 2002 09:31:58 -0700

In order to monitor the U.S. civilian population in its effort to detect terrorists, the government's Total Information Awareness program will rely almost completely on data collection systems that are already in place -- e-mail, online shopping and travel booking, ATM systems, cell phone networks, electronic toll-collection systems and credit card payment

terminals. Technologists say that what the government plans to do in data sifting and pattern matching in order to flag aberrant behavior is not very different from programs already in use by private companies. For instance, credit card companies use such systems to spot unusual spending activities that might signal a stolen card. The early version of Total Information Awareness uses a commercial software collaboration program called Groove, which was developed in 2000 by Ray Ozzie, inventor of Lotus Notes. Groove enables analysts at various government agencies to share intelligence data instantly, and links programs that are designed to detect suspicious patterns of behavior. However, some computer scientists question whether such a system can really work. "This wouldn't have been possible without the modern Internet, and even now it's a daunting task," says cryptology expert Dorothy Denning, a professor in the Department of Defense Analysis at the Naval Postgraduate School. Part of the challenge, she says, is knowing what to look for. "Do we really know enough about the precursors to terrorist activity? I don't think we're there yet." [*The New York Times*, 23 Dec 2002; NewsScan Daily, 23 December 2002]
<http://partners.nytimes.com/2002/12/23/technology/23PEEK.html>

✶ The Total Information Awareness program is a RISK!

Edward G. Nilges <spinoza1111@yahoo.com>
26 Dec 2002 15:34:36 -0800

In *The New York Times* for 23 Dec 2002, John Markoff and John Schwartz find that "Many tools of Big Brother are up and running."

In this article, they describe how the Total Information Awareness or TIA program hopes to use the extended Markup "Language" (XML) as a form of Krazy Glue to create the mathematical union of existing and wildly disparate data sets.

Quite apart from genuine concerns about privacy, the real problem may be correctness.

This is because the "end user's" vision of a data base, as opposed to a large program, is relatively optimistic. Intelligent end users know in some way the Turing pessimism: that there is no automated procedure, and often no practical procedure, for determining whether a large software artifact "halts" or more generally arrives at a desirable state.

But what they may not know is that modern data bases including Oracle and SQL Server include meta-data that in effect transforms the non-Turing-complete (and therefore controllable) data base into a very large Turing machine.

This meta-data traditionally consisted of format declarations, which do not in themselves present the Turing problem, but also consists of "stored procedures."

These are modally small but sometimes large programs written in a Turing-complete programming language that have the ability to form part of

the semantics of the data base.

For example, a yes/no flag (indicating "probable terrorist involvement") may be accessed via an automated trigger that returns not its raw value, but its value, ANDed with another flag that overrides the raw flag. The latter flag may indicate an explanatory condition such as association with organizations already known to be neutral (such as the Red Crescent), which association lowers the probability of the original condition.

And, although traditional meta-data (such as the use of Long or 32-bit representation for an integer value) does not make a data base Turing incomplete it may (or may not) represent a statement about the data.

The selection of 32 bits may represent a decision that the value in question ranges between -2^{31} and $-2^{31}-1$, or it may represent ONLY the absence, at the time the data base was created, of a 64 bit architecture.

The problem is that eXtended Markup Language CAN represent all these subtleties in principle but WILL NOT in practice owing to time pressures. Already in the literature one finds a split. Managerial articles on XML promise complete control, while in the same journal, programmers and system administrators are assured that XML is permissive and will allow the representation of values as ASCII strings...without type constraints.

XML is no Pascal but is instead in the tradition of C, which allows the developer to make forensic decisions on his own without

oversight. The manager believes that everything is under control, while in the server room it is decided, modally in an undocumented way, that a citizen who posts long articles on the Internet is a potential troublemaker.

The problem is that the artifact resulting will be an uncontrollable, because Turing complete, PROGRAM that will form its own documentation.

As a form of de facto electronic law, it will result in even more Constitutional mischief than we've seen enough of already in the war against terrorism.

✶ Old mechanical voting machines also break, but have audit trails

danny burstein <dannyb@panix.com>
Sat, 7 Dec 2002 18:15:11 -0500 (EST)

We've got a curious case in White Plains, NY (about 20 miles north of NYC) in which one of the older mechanical voting machines broke down - leading to a great deal of messiness as to who won the election. The allegation is that the lever for one candidate jammed, so people couldn't readily vote for him. The good thing here is that there was feedback to the voters that they weren't getting through and that these concerns were, indeed, taken seriously. (We all know far too well the problems with more "modern" systems).

For various legal reasons the losing candidate doesn't have direct standing, but has to defer to the Attorney General. Mr. Spitzer's office investigated, and has now filed the court paperwork.

to quote from the AG's press release:

"In March, Delgado requested that the Attorney General consider bringing a *quo warranto* action. Following long-standing office policy, the Attorney General's Office convened a panel of three seasoned assistant attorneys general to investigate the White Plains Common Council election. During its six-month investigation, the panel interviewed Delgado and Hockley, as well as officials from the Westchester Board of Elections and poll workers.

"Information uncovered in the investigation showed that the voting machine in the 18th Election District had, in fact, jammed only on the line with Delgado's name, preventing votes for him from being recorded. In the investigation, the panel received 103 sworn affidavits from White Plains voters who said they voted for Delgado on the voting machine in the 18th Election District. The investigation also determined that those voters had signed in and voted at the 18th Election District. Those 103 votes would have been more than needed to overcome the 47-vote differential between the candidates. [...]

So while it's taking much longer than I'm sure anyone would like, the process is clearcut and making its way through.

further details at:

http://www.oag.state.ny.us/press/2002/dec/dec03c_02.html

✶ **Electronic vote machines open to tampering - report**

Derek Harnett <dharnett@eurologic.com>

Mon, 9 Dec 2002 13:34:44 -0000

In the last couple of elections/referenda here we've had a few pilot schemes here for electronic voting. The plan is to introduce electronic voting countrywide in the next couple of years. The system is one that does not have an paper audit trail etc. Despite commissioning an report on the integrity/security of the systems used, the government department responsible seems set on ignoring the results of the report and will continue to roll out the process.

>From the 'Irish Independent' 9 Dec 2002:

Electronic vote machines open to tampering - report

A PRIVATE report for the Department of the Environment has cast doubt on the security of the ballot in new electronic voting machines.

The "powervote" machines, deployed in seven constituencies at the last general election and due to be used countrywide for the local and European elections in 2004, are vulnerable to tampering, the report claimed.

Consultants Zerflow told the department that it would be easy to

paste a dummy ballot paper over the face of the machine, rearranging the list of candidates, in a bid to attract votes away from someone perceived as likely to be the most popular candidate.

The examination team also successfully obtained a key to operate one of the machines and copied it at a local shopping centre - raising the scenario of tamperers armed with many keys reactivating the machines after close of voting to engage in the electronic equivalent of ballot-stuffing.

The Department of the Environment has rejected many of the concerns, pointing out that the machines' integrity is protected by a scrutineer who remains by each machine during voting.

Fine Gael spokesman Bernard Allen said last night that the Minister for the Environment, Martin Cullen, must now publish the full facts relating to the Zerflow report.

He said he would be asking the Chairman of the Oireachtas Environment Committee to convene a meeting to examine the situation in detail. The report's authors and the minister would be invited to discuss the matter.

"There should be no further consideration given to extending electronic voting until such time as the system can be guaranteed to be secure," he said.

The report identified several "high level" risks to the integrity of the vote, and suggested that results obtained under the current

system could be
open to legal challenge.

Powervote said its machines have been operating in Germany and
the
Netherlands for over a decade without problems.

✶ Is a cleared check really like money in the bank?

"Sidney Markowitz" <sidney@sidney.com>

Thu, 19 Dec 2002 00:41:15 +1300

Wired has an article on a new Nigerian scam

<http://www.wired.com/news/culture/0,1284,56829,00.html>

The con can be abstracted into these steps:

1. Con artist sends you a cashier's check as payment for something.
2. Some reason you find plausible is given for you to send back a portion of the money once you are sure that the check has cleared
3. You deposit the check, wait until the bank says it has cleared, and send some part of the money to the con artist
4. Bank informs you some days or weeks later that the check was a counterfeit and you owe them the full amount they paid you

There seems to be a really big RISK here, aside from the Nigerian scam: It is common for check transactions to be held until the check clears, to ensure that the check is good. Now we see that the time it takes for a check to clear is determined by US law that sets a limit on how long a

bank can delay paying for a deposited check. But that limit does not make it any faster for the bank to really determine if the check is good. The unintended consequence of the law is that a cleared check may not be a cleared check, with the depositor being the one who is liable if something goes wrong.

⚡ Baffling ATM behavior

Bill Bumgarner <bbum@codefab.com>

Wed, 11 Dec 2002 15:03:27 -0500

Yesterday, I stopped by an ATM to pick up a bit of cash and experienced a truly stupid bit of interaction with the ATM.

I inserted and retrieved my card, typed my PIN, typed the amount of money I wanted, agreed to pay the vig, and hit enter to receive my cash.

Nothing.

No warning, no beeping, no error message, no cash. No feedback whatsoever.

Then I noticed that the machine had the previous customer's receipt sticking out of the printer slot. Assuming it wouldn't help, I removed the receipt.

Lo and behold, the machine coughed up my cash, coughed up a receipt (that I didn't ask for), and the transaction was concluded.

The risks should be obvious:

- Machine enters a 'locked' state after concluding the transaction internally, but before cash is delivered to user
- Zero feedback of what is holding up transaction completion
- Spitting out a receipt when the user explicitly asks NOT to receive a receipt

I would assume that the system completes the transaction with the user's account immediately prior to dispensing cash. As such, the cash to be dispensed is "in the queue" and no longer in the account?

The potential scam is much more nefarious. It would be trivially easy to use a razor to cut off the receipt in the printer slot after a transaction is completed. Once done, the thief merely has to wait for someone who tries to obtain cash, but isn't aware that the machine will lock up in the fashion described above. The user will eventually walk away-- maybe pressing cancel, more likely not (I didn't test that the 'cancel' would really 'cancel' the transaction). Given that the ATM is on the side of the bank that owns the ATM, it is quite likely the user will step into the bank for assistance.

As soon as the user steps away, the thief merely has to extract the old receipt to cause the machine to spit cash.

It would be hard to even prove that the thief was actually a thief and not someone who just lucked into completing the transaction.

I'm certainly going to check twice that the printer slot is

clear before
using any ATM, but I can think of a number of situations where a
blockage
wouldn't be visible.

[Correction inserted in archive copy. PGN]

✦ **Re: Crackers steal 52,000 university passwords ([RISKS-22.39](#))**

Harald Hanche-Olsen <hanche@math.ntnu.no>

Sun, 01 Dec 2002 01:00:19 +0100

Regarding the break-in where crackers stole the password file
from the
University of Oslo [[RISKS 22.39](#)], the mere fact that they
managed this isn't
half as interesting as the reason they could pull it off.

Apparently, the crackers got in via a computer used for testing
a new
administrative system for the telephone exchange. As it turns
out, this
system is based on the MS SQL server, a fact unknown to the
people
installing the software. Now they had installed the latest
security patches
for the whole system, except for the SQL server - since they
were not aware
that it was running. And that provided the crackers' opportunity.

✦ **Why you should read Mitnick's book: The risks of seeing the trees**

"Don Norman" <don@jnd.org>

Wed, 18 Dec 2002 02:46:21 -0600

and not the forest

In an apparent coincidence, in [RISKS 22.43](#), in the article that followed my recommendation that RISK readers read the new book by Mitnick & Simon, Rod Slade did his standard "this book has no merit" review of the book.

Slade is wrong: you should read this book.

Slade criticizes each individual tree, and thereby misses the forest.

His critique of the individual trees is correct. Are the stories repetitive? Yes. (you know, each tree looks just like the other, and after awhile, it gets boring.) Is the book self-serving? Yes. Is Mitnick reformed or still a scoundrel (guess). Is the advice he gives rather pedestrian or even worthless? Yes. Are there any new, profound insights, well, no, not if you keep your head down and only focus on the trees.

But individual trees add up to a forest, and there is value in studying forests.

I'm a student of human psychology. That's what I do for a living.

Technology and people. Among other things, I read books by ex-criminals:

Thieves, bank robbers, con-artists. I learn a lot. This is not the first such book I have read. And it won't be the last.

I learned a lot from Mitnick. I was impressed by his approaches. They are not as simple and easy to do as a quick reading would make

them
appear. After the fact, everything always looks obvious. But I,
for
example, would find it difficult to even think of the schemes,
let alone
carry them out successfully. As with all great confidence
operators, he
knows a lot about practical, human psychology. He knows how to
set up
the mark. How to make multiple phone calls or visits, each to a
different person, each asking for help, and each time picking up
one
little piece of information that, by itself, does not seem
important.
How to win confidence. And then, put the little bits together,
and you
sound like a legitimate employee, supplier, or customer in an
unfortunate situation, where just a little help would be
useful. It's
classic con-artist, and he does it very well.

I believe that many readers of RISKS would learn a lot -- and be
very
bothered by what was learned; it would be very easy to fall for
some of
those ruses. (As Mitnick points out, even good con artists will
sometimes fall for other people's cons.) This is a really good
antidote
to all those technical approaches to security.

Slade also can't decide how to treat Mitnick: as a weak
technologist
(hey, most of his cons don't involve technology, so what's the
big deal)
or as too good a technologist (to do one fraud, you need to
reprogram a
DMS-100 switch). That last fraud, by the way, is quite
interesting: Go
out and buy a used switch -- or just get access to someone
else's -- and
you can make the telephone caller ID say anything you want it
to. So
don't trust caller ID to show that the caller is someone you

know, or
from your own company. Is this news to professionals? No. Is it
good to
know? Yes. Would a serious person trying to steal company
secrets, or
money, use the trick? Gee, I would -- wouldn't you? Of course
they
would. Can I program the switch? No, but I could learn, or more
easily,
just hire someone to do it for me.

Slade complains that this is not a technology book, "this is a
book
about how to fool people." Well, yeah, duh, that's the point.
Put up all
the technology you want, it isn't that secure because I'll break
in from
inside, or fool people into giving me the information I seek.

So, if you are a security professional, you can ignore the book.
Maybe.

You already know all this stuff. You could probably write a
better book
yourself. If you aren't such an expert, read the book. Its an
easy read.

Big print. Lots of stories. No big words or deep thoughts. Very
repetitive. But I found it revealing -- and frightening.

On one thing Slade and I agree: "Chapter four tells you to
distrust
everyone--which would probably be more damaging to society than
social
engineering." Yup, this was precisely the point of my posting in
RISKS
22.43. It is already becoming more damaging.

Read Mitnick & Simon. Don't take their recommendations seriously
-- they
are lightweight, sometimes wrong or irrelevant, and probably
there for
legal reasons -- to impress the court that this is a prevention
book,
not a "how-to" book.

It's a great how-to book, and if you read it, you will become better at prevention. Maybe.

Don Norman, Computer Science, Northwestern University <http://www.jnd.org>

Nielsen Norman Group <http://www.nngroup.com> norman@nngroup.com

🔥 Surgical tool left in woman's stomach for 4 months

Keith Rhodes <rhodesk@gao.gov>
Tue, 17 Dec 2002 08:31:52 -0800 (PST)

An airport metal detector was triggered by a Canadian woman, although no metal was evident. Noting that she had been suffering from persistent stomach pains ever since abdominal surgery, she went for an x-ray the next day. A four-inch surgical retractor was discovered in her abdomen.

[CNN.com, PGN-ed]

[BROKEN URL:

<http://www.cnn.com/2002/WORLD/americas/12/16/canada.woman.stomach.reut/index.html>

TRY

<http://www.hon.ch/News/HSN/510912.html>

which says it was a 33-centimeter retractor.

NOTE ADDED in archive copy. PGN]



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 45

Weds 1 January 2003

Contents

- [Hard-coded calendar dates](#)
[Dave Stringer-Calvert](#)
 - [Somebody stole backup tapes containing citizen's private information](#)
[Ishikawa](#)
 - [Poor encryption: Transportation Security Administration](#)
[M Taylor](#)
 - [Browser incompatibilities cost business](#)
[Geoff Kuenning](#)
 - [No such thing as "knowing that a check has cleared?"](#)
[Daniel P.B. Smith](#)
 - [Re: O Big Brother, where art thou?](#)
[Edward G. Nilges](#)
 - [Re: Why you should read or should not read...](#)
[Fred Cohen](#)
 - [REVIEW: "Software Engineering", Ian Sommerville](#)
[Rob Slade](#)
 - [REVIEW: "Trusted Computing Platforms", Siani Pearson](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ Hard-coded calendar dates

Dave Stringer-Calvert <dave_sc@csl.sri.com>

Wed, 01 Jan 2003 12:45:28 -0800

The front page of the *Yorkshire Evening Press* Web site (<http://www.thisisyork.co.uk>) is declaring today to be Wednesday, January 1 2002. The JavaScript on the page is:

```
document.write(dayNames[day] + ", " + monthNames[month] + " " +  
date + ", 2002");
```

Happy *NEW* year!

Dr Dave Stringer-Calvert, Assistant Director, Computer Science
Laboratory

SRI International, Menlo Park CA 94025-3493 1-650-859-3291

✶ Somebody stole backup tapes containing citizen's private information

Ishikawa <ishikawa@yk.rim.or.jp>

Tue, 31 Dec 2002 00:50:48 +0900

I would like to report an incident which made me feel dizzy at this otherwise tranquil days at the end of the year.

In Japan, a national system to coordinate citizen's private information stored in government computer is being prepared amid vocal opposition from various parties.

Basically, a single number, 11 decimal digits number is assigned to each

individual and this will be used as the search key in accessing various data bases. (Some kind of mapping table would be prepared by local government agencies with this nationally unique number to access individual's record in local government databases .) There would be a nation-wide network where the key would be used as the primary key for accessing various databases scattered across the nation.

The danger for abuse is obvious and the fear is so much that some cities and jurisdictions decided to challenge the national policy by declaring that they would not be online with the system, etc. when the final preparation for the full-scale deployment began this summer. (The city of Yokohama where I live decided to allow the citizen to decide if the personal number assigned to them would be delivered to the prefectural level data center or not unless sufficient assurance for protection is forthcoming from the national government. About 30% of the population asked the number not be sent, and this popular demand made national newspaper headlines : Yokohama has about 3 million population and is a big city in Japanese scale of things. Obviously the government agency which is pushing the national policy and the construction of the network has PR problems now.

The risk is now huge since the diet (national parliament) failed to enact a privacy protection law which should have been prepared along with such a numbering system.

Anyway, the national government has been trying to assure that

the system
would be safe with computer security protection, etc..

However, it has already been criticized for such mundane thing
as slow
anti-virus data update which would take place once a few months
(!) [makes me
wonder where on earth they have been living in the last few
years.], which
the government agency claims is not a serious threat since the
network in
question is not directly connected to Internet, etc.. But, of
course, some
town offices seem to use the same computer for internal LAN and
accessing
the national network in question. (There must be some form of
physical
switches in place, but we never know what happens. Murphy's law
always
strikes.)

Probably the last straw which might break the pro-numbering
support is the
theft of backup magnetic tapes that happened in a town north
east of Tokyo.

There, five backup DAT tapes of the town office computer systems
containing
privacy data of approximately 9600 were stolen from a parked car
of a
computer maintenance service company. The tapes were on the way
for off-site
storage, and were in a metallic attache case. It seems that
whoever stole
the case mistook it for one containing money or some other
valuables. (On
the other hand, since the parking lot belongs to the computer
maintenance
company, we should not rule out that a serious cracker (or two?)
stole the
tapes to gain foothold into the national network.)

The newspaper articles aren't clear what are on the tapes and in

what form,
but the city spokesman stated that the data did include the national numbers for the citizens and privacy data such as address, name, gender, birth date, qualification status for the various national health insurance plans, and pensions. The data is claimed to be in encrypted form (but no detail) and won't be easy to read according to the statement. However, given the risks, the city officials decided to ask the permission of each citizen to change the numbers assigned to them so that the numbers themselves won't be used for some malicious tampering in the future. (The law requires that the change of numbers needs the consent of the citizen.)

Numbers aside, the rest of the information, if decrypted, would be the staggering source for privacy theft, etc.

I can't say for sure but some say that backups were made using ARCserver backup software or something. I have no idea what type of cryptography it supports, but I surely hope the algorithm is a good one and the key length is long enough if ARCserver is indeed used for this national network.

The tapes were stolen on 26th, and found scattered on a river bank on 30th.

Three tapes were found outside the opened metallic case. The lock to the attache case was forced open. (So two of the DATs were still missing, it seems. Again the newspaper article that I read was not very clear on this point.)

Using encryption for backup data is a common sense. But then I

have no idea
how the key for the encryption is managed and what type of
algorithms are
used in this particular case, and if I were the citizen of the
town of
Iwashiro, I would have been disturbed very much.

One thing I don't like about this national network being built
is the
apparent lack of security policy.

Since there is no clearly written national security policy, this
type of
problems, like the maintenance person leaving the valuable data
tape in an
attache case inside a car parked at company parking lot, may
happen in the
future. The way the network is built and the apparent lack of
nation-wide
security policy of this network force me to think that
information leak
caused by computers that are linked to the network and also have
outside
connection inside the town/city office LAN, which in turn, may
have
unexpected Internet link via somebody's modem, or even caused by
simple
eavesdropping via wireless LAN may happen not in the distant
future.

I hate to think that the government has to go through such
incidents before
learning the basic of security management.

After writing this, I realize the above may look unbelievable to
security
consultants who read Risks today, but is true and is happening
now in Japan.

Only in the last few months, some government agencies learned
the danger of
wireless LAN: some drive-by inspection caught the contents of
the unencrypted

traffic easily.

I hate to think about the mess caused by large-scale identity theft, etc..

This incident of stolen tapes wiped out the last trust I had in this national numbering system and I am no longer in the mood of festive holiday season.

✂ Poor encryption: Transportation Security Administration

M Taylor <mctaylor@privacy.nb.ca>

Tue, 31 Dec 2002 16:07:21 +0000

TSA Documents' Protection Easily Circumvented

Several restricted U.S. Transportation Security Administration (TSA)

documents are accessible to anyone with an Internet connection. While

they are password protected within Microsoft Word, once they are downloaded, they can be attacked with password cracking software at the user's leisure.

[Source: reuters 24 Dec 2002, in SANS NewsBites, 30 Dec 2002, Vol 4 no 53]

<http://reuters.com/newsArticle.jhtml?type=internetNews&storyID=1958544>

So how risky is it to provide insecure "encryption", that misleads users into thinking that their documents are safe? It appears to be RISKY for the user, to rely on such labelled "features" in the software they choose to use.

M Taylor <http://www.mctaylor.com/>

[Geoff Kuenning noted this quote in the article:

"We think it's safe," a spokesman said. "From our standpoint it's very workable and secure."

PGN]

Browser incompatibilities cost business

Geoff Kuenning <geoff@cs.hmc.edu>

Mon, 30 Dec 2002 04:13:25 -0800 (PST)

I have noticed a trend in the past 6 months of increasing numbers of Web sites that will not work correctly with my browser. The most common symptom is a blank page, presumably because some bit of JavaScript failed to execute the way they assumed it would. (In one case, I took the trouble to diagnose the failure and found that a null URL was expected to load the referring page; replacing it with a proper URL cured the problem.)

What amazes me is that most of these bugs are caused by unnecessary use of new (i.e., not widespread) features, and that they cost companies business. For example, this evening I tried to buy Kevin Mitnick's book, as recommended by Don Norman in RISKKS. Try as I might, I could not get buy.com's site to allow me to enter an updated credit-card number. I finally gave up, started the search over, and purchased the book elsewhere.

One has to wonder how much business has been lost because gadget-loving programmers are more fascinated with the latest features than with compatibility.

Geoff Kuenning geoff@cs.hmc.edu <http://www.cs.hmc.edu/~geoff/>

⚡ No such thing as "knowing that a check has cleared?" (Re: [RISKS-22.44](#))

"Daniel P. B. Smith" <dpbsmith@bellatlantic.net>

Mon, 30 Dec 2002 07:05:40 -0500

In reference to a Nigerian scam, "Sidney Markowitz" <sidney@sidney.com> says that "It is common for check transactions to be held until the check clears, to ensure that the check is good. Now we see that the time it takes for a check to clear is determined by US law that sets a limit on how long a bank can delay paying for a deposited check. But that limit does not make it any faster for the bank to really determine if the check is good. The unintended consequence of the law is that a cleared check may not be a cleared check."

Some years ago I once was in a situation where I wanted to be certain that a check "was good" and "had cleared."

I had a lengthy discussion with a bank vice-president, and I understood him to say that the clearinghouse system does not provide any way to ever know for certain that any particular check has cleared. If a check FAILS to clear, everyone finds out about it. But when a check clears successfully, there is no traceable information about the transaction. He

said that,
theoretically, there was no way to know that a particular check
had cleared.

I was told that it "was safe to ASSUME" that if the check had
not bounced
within two weeks, that it "must have cleared," but that there
was no
positive guarantee and no way to check the status of any
particular check.

Daniel P.B. Smith dpbsmith@world.std.com dpbsmith@alum.mit.edu

[Similar comments from Brian Reynolds ("This is not a new
scam."), Tony

Lima, Ron Bean ("Could be a big risk for banks as well, given
their

Clinton-esque definition of the word "cleared"). PGN]

🔥 Re: O Big Brother, where art thou? ([RISKS-22.44](#))

Edward G. Nilges <spinoza1111@yahoo.com>

1 Jan 2003 12:33:12 -0800

I would strengthen Dorothy Denning's objections, for they
redescribe
terrorist surveillance as a "daunting task."

Unfortunately this shares with the TIA the assumption that the
task, of
surveillance, is one that can be solved at all.

The literary critic, and Palestinian moderate activist, Edward
Said, has
pointed out that the US State Department tends to hire people
with easily
measured skills in development economics to work on Mideast
problems. He

has contrasted this with the older practice of Britain's foreign and colonial desks, which was to hire literary dons who had specialized in topics such as Persian poetry.

The most recent example of this mindset was the termination of several Arabic speakers at the Defense Language Institute because of their sexual orientation; for there is a linkage between hatred of "soft" skills and homophobia.

There are drawbacks to both practices, but Said does point to a bias...in favor of the technological quick fix of which the Total Information Awareness program is an example.

Furthermore, solid technical arguments lead one to conclude that the TIA will not work.

First of all, Groove is a commercial software product, and, if my guess (that the TIA is in part a bit of a bailout for Bush's friends in the IT industry, suffering as it is in a depression), the design of the TIA will emphasise commercial and off-the-shelf solutions.

The problem is that this MEANS that the ill-defined "enemy" can acquire the same software being used to surveille him, run it to detect what it, in turn, detects, then change his patterns. In a sense, a Turing machine (the Groove system running on TIA computers) is examining a social Turing machine (the bad guys and their copy of Groove) to see whether it will arrive at a "halt" state (an attack.)

This Turing problem is independent of hardware and software. We can be certain that terrorists will no longer try to carry box cutters on board airplanes and overwhelm the passengers and crew in what seems a "conventional" hostage situation but what is a suicide attack, for such behavior will now be coded, by the passengers, as a suicide attack.

Unfortunately, Professor Denning's objection, that it's a "daunting" task, can be met by the language of go-ahead problem-solving in which the person who says it's a "daunting" task is placed at a disadvantage, rhetorically. She makes it sound as if we're not up to it.

Unfortunately, negative results (such as Turing's) stay true and are not disproved by technical progress, any more than perpetual motion becomes true.

In algorithmic terms, a "computer" (the US defense establishment) is examining another "computer" (al-Qaeda) to find its halt state, and, to complicate matters, the examinee knows of the monitoring.

Even if a data base existed with full optics and sound that replicated ALL activity in Eurasia alone, any one action could, or might not, be an encoding of terrorist intelligence and for this reason, interpretation would become the job of the same people who failed to bring in the "twentieth hijacker" for questioning. Our government would have to refute, at the level of basic science, Alonzo Church's thesis to the effect that all

computers are Turing machines, and it would have to make or buy a Turing+n system that could defeat other Turing+0 systems.

Nor can our government "scale up" for adding cycles doesn't change the math.

The near-demise of supercomputing as big iron shows us that the bad guys can use networks in place of centralized big iron.

Of course, this is the point at which truly rational men and women throw

down their gear and advance across wastelands with ancient symbols of peace.

This is the point at which Ronald Reagan, a quite ordinary man, abandoned

the equivalent insanity of Mutual Assured Destruction and went to Reykjavik.

However, what American politician has the courage to solve the Mideast

problem by raising our gasoline taxes, and announcing that the US should be

considered an alternate homeland for Jews worldwide (boy, that was easy)?

The problem is that the United States is engaged (like it or not) in a

dialogue with terrorists. If like Sharon in Israel and Cheney here, our

statesmen play to the gallery, and "refuse" to "dialog" with "terrorists",

they discover that violence becomes the language of choice.

"Hackerz" already change the spelling of code words faster than they can be

defeated by scanners. Unless the US develops (at considerable expense) a

proprietary technology-of-surveillance which cannot be reverse engineered,

the TIA is at best a boon doggle and at worst a replacement for a needed

dialog.

✂ Re: Why you should read or should not read... (Norman, [RISKS-22.44](#))

Fred Cohen <fc@all.net>

Mon, 30 Dec 2002 08:23:25 -0800 (PST)

Why not read the book?

Because the author is a con artist and you are sending him \$s?

OK - so Don makes the point that:

"I'm a student of human psychology...

I read books by ex-criminals:...

I learn a lot."

Fair enough. If you are studying criminal behavior, reading books by crooks is probably a good idea. But if you want to know about cons, far better books are:

"Flim-Flam" by James Randi

"Scam School" by Chuck Whitlock

and "Rip-Off" by Fay Faron

All three are by legitimate researchers who present results taken from scores to hundreds of incidents and present how and why scams work, the techniques used, the different plots, and so forth. They present many excellent examples of how these sorts of crimes work, how they impact the victims, the psychology of the criminals, and so forth.

> I learned a lot from ... I was impressed by his approaches. They

> are not as simple and easy to do as a quick reading would make

them
> appear. After the fact, everything always looks obvious. But
I, for
> example, would find it difficult to even think of the schemes,
let alone
> carry them out successfully.

One of the major problems we face in information protection is
people who
just don't think cleverly of bad things that could happen. It
might serve
Don well to take an introductory course in the subject matter.
He will
learn a lot more than from a book by a crook and he will be
supporting
defenders rather than attackers.

Fred Cohen - <http://all.net/> - fc@all.net - fc@unhca.com
tel/fax: 925-454-0171 Fred Cohen & Associates - University of
New Haven

🔥 REVIEW: "Software Engineering", Ian Sommerville

Rob Slade <rslade@sprint.ca>
Tue, 24 Dec 2002 08:17:04 -0800

BKSFTENG.RVW 20020916

"Software Engineering", Ian Sommerville, 2001, 0-201-39815-X, C
\$104.95

%A Ian Sommerville ian@software-engin.com

%C P.O. Box 520, 26 Prince Andrew Place, Don Mills, Ontario
M3C 2T8

%D 2001

%G 0-201-39815-X

%I Addison-Wesley Publishing Co.

%O C\$104.95 416-447-5101 fax: 416-443-0948

%O <http://www.amazon.com/exec/obidos/ASIN/020139815X/>

[robsladesinterne](#)

%P 693 p.

%T "Software Engineering, Sixth Edition"

Part one is an overview. Chapter one is an introduction, a FAQ (Frequently Asked Questions list), definitions, and, interestingly, a section on ethics. A broad review of system development concepts (such as emergent properties) is presented as computer based software engineering, in chapter two. Stages in the software development process, none detailed, are listed in chapter three. Project management is discussed in chapter four.

Part two looks at software requirements. Chapter five examines different types of requirements. Requirements engineering is software engineering in miniature, as chapter six points out. There is a heavy emphasis on the Universal Modeling Language (UML) in chapter seven's explanation of system models. The benefits and dangers of software prototyping are examined in chapter eight. Chapter nine points out that formal specification does require special training on the part of users, but can identify problems in requirements specifications. (More extensive examples would be helpful in making this point more convincing.)

Part three reviews design, and the chapters are mostly divided by system type. Chapter ten explains architectural design, and reviews tools and models. (Security, and other concerns, are addressed throughout the book: an example in this chapter points out that interrupt driven architectures are complex and difficult to validate.)

Distributed systems architecture itself gets oddly short shrift in chapter eleven, which concentrates on client/server and CORBA (Common

Object Request Broker Architecture). Object-oriented design is shown to be very much like modular design in chapter twelve. (The stated objective of the text is to introduce UML, but the explanations are not very clear.) Chapter thirteen looks at real-time software design but does not seem to be as complete as other topics. Design with code reuse is a good overview, but chapter fourteen starts out with the statement that electrical and mechanical engineers rely on component reuse, ignoring the lack of a broad range of standard components in the software environment. There are good, basic suggestions for user interface design, in chapter fifteen, although the discussion is limited. For example, the recommended principles suggest confirmation of destructive actions, but don't note the fact that even such confirmations become automatic over time, and therefore are not particularly useful.

Part four deals with critical systems. Chapter sixteen looks at dependability in terms of availability, reliability, safety, and security. Critical systems specification, in chapter seventeen, examines dependability (and failure) metrics. Risk analysis is discussed, but not in the usual combination of probability and severity. Critical systems development is examined both in terms of fault avoidance and fault tolerance in chapter eighteen.

Part five covers verification and validation. Chapter nineteen concentrates on code inspection and the Cleanroom process. Software testing, in chapter twenty, looks at types, cases, and procedures. Critical systems validation, in chapter twenty one, is basically the same process as the previous chapter, but more important.

Part six, on management, is mostly a precis or list of principles from other sections. Chapter twenty two deals with managing people, looking at limits, motivation, group dynamics, recruiting, and keeping, as well as a quick overview of the People Capability Maturity Model (P-CMM). It's not a large section, but it is nice to see the importance of personnel recognized in this way. Software cost estimating, in chapter twenty three, is interesting, but possibly not terribly useful. Quality management is dealt with in chapter twenty four. Chapter twenty five reviews process improvement and the Capability Maturity Model (CMM), mentioning the work of Walter Deming but not, intriguingly, dealing with the fact that Deming's later work suggested that business had gone overboard in the pursuit of quality.

Part seven deals with evolution and change. Chapter twenty six discusses legacy systems with a description of mainframe program structures and guidelines for the assessment of the possibilities for updating the system. Software change is reviewed in chapter twenty seven, with maintenance and re-architecting leading to a description of re-engineering in chapter twenty eight. Chapter twenty nine finishes off with configuration management, emphasizing version documentation more than change control.

The book is written as a textbook, with a summary of key points and a very decent set of exercises at the end of every chapter. It certainly stands above the other systems development texts that I have experienced. However, this work also has value beyond the classroom.

A great many professionals, such as information security officers, need to know the operations, procedures and concepts of software

engineering without necessarily being programmers themselves.
For these people, this volume makes a clear and excellent reference.

copyright Robert M. Slade, 2002 BKSFTENG.RVW 20020916
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

<http://victoria.tc.ca/techrev> or <http://sun.soci.niu.edu/~rslade>

★ REVIEW: "Trusted Computing Platforms", Siani Pearson

Rob Slade <rslade@sprint.ca>
Fri, 27 Dec 2002 08:02:27 -0800

BKTRCMPL.RVW 20020916

"Trusted Computing Platforms", Siani Pearson, 2003, 0-13-009220-7,

U\$49.99/C\$77.99

%E Siani Pearson

%C One Lake St., Upper Saddle River, NJ 07458

%D 2003

%G 0-13-009220-7

%I Prentice Hall

%O U\$49.99/C\$77.99 +1-201-236-7139 fax: +1-201-236-7131

%O <http://www.amazon.com/exec/obidos/ASIN/0130092207/>

[robsladesinterne](#)

%P 322 p.

%T "Trusted Computing Platforms: TCPA Technology in Context"

Part one introduces trusted platform technology, as a kind of public key infrastructure implemented in hardware. (Which begs the question: what do you do about key revocation?) Chapter one, an overview of the trusted computing platform concept, is not very clear on basic

ideas

beyond hardware implementation involvement and the notion of measurement, or assurance. There are usage scenarios of applications

that can be done, or done better, with trusted platforms, in chapter

two. Not all of these cases are convincing evidence that trusted platforms are better. The cryptographic underpinnings of trusted platforms are examined in chapter three, but it would be clearer if

the basics of asymmetric cryptography were covered and standard cryptographic and certificate authority terms were used.

Part two concerns trust mechanisms in a trusted platform, but is basically a list of commands. Chapter four deals with access control,

to do with physical presence requirements, ownership, and authorization. Platform identification and endorsement is covered in

chapter five. Chapter six discusses integrity recording, reporting,

and secure boot. Protected storage of keys is in chapter seven, migration and maintenance methods in chapter eight, and other assorted

functions in chapter nine.

Part three reviews trusted platforms in practice and operation.

Chapter ten describes the setup of a new trusted platform, chapter

eleven deals with what would elsewhere be known as trust relationships, and challenging a trusted platform-- authentication of a

server--is in chapter twelve.

Part four presents the benefits of trusted platforms, first to organizations and corporations, in chapter thirteen, and then to individuals and users, in chapter fourteen.

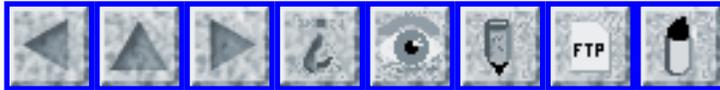
This book is not clear, either about what TCPA (Trusted Computing Platform Alliance) technology is, nor how it can effectively be used.

Although the authors occasionally admit that there may be problems

with the system, there seems to be a kind of background arrogance in operation, that assumes everyone will have to use this technology, so they might as well learn the commands.

copyright Robert M. Slade, 2002 BKTRCMPL.RVW 20020916
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

<http://victoria.tc.ca/techrev/~rslade> or <http://sun.soci.niu.edu/~rslade>



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 46

Friday 3 January 2003

Contents

- [H&R Block employees suspected of identity theft against 27 customers](#)
[Monty Solomon](#)
- [Half-million people victimized by stolen hard-drives](#)
[Monty Solomon](#)
- [Woman shot by former classmate who stalked her by Internet](#)
[Monty Solomon](#)
- [Man allegedly stalks ex-girlfriend with help of GPS](#)
[George Mannes](#)
- [Credit agencies provide information on your relations under DPA](#)
[Tim Storer](#)
- [PGP.COM cannot handle sales to some US residents](#)
[Michel E. Kabay](#)
- [/Trivial/ Risks of Technical Arrogance](#)
[melandrob searle](#)
- [Oregon proposing taxing in-state car mileage via GPS](#)
[Mike Hogsett](#)
- [Re: Total Information Awareness / O Big Brother](#)
[Fredric L. Rice](#)
- [Re: Computer programmer faces U.S. fraud charge](#)
[Bob Morrell](#)

- [Re: Surgical tool left in woman's stomach for 4 months](#)
[John Sullivan](#)
 - [Caller ID untrustworthy](#)
[Mathew Lodge](#)
 - [REVIEW: "Protect Your Digital Privacy", Glee Harrah Cady/Pat McGregor](#)
[Rob Slade](#)
 - [REVIEW: "Privacy Defended", Gary Bahadur/William Chan/Chris Weber](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ H&R Block employees suspected of identity theft against 27 customers

Monty Solomon <monty@roscom.com>

Thu, 2 Jan 2003 16:12:19 -0500

A federal complaint charges that 27 people who went to H&R Block for help with tax preparation through April 2001 had their personal information stolen in an identity theft scam involving four suspects, who allegedly used names, addresses, SSNs, and dates of birth to alter the victims' addresses for tax refunds, opened new credit-card accounts, etc. H&R Block reportedly would not cooperate in the investigation until it was subpoenaed. [Source: Associated Press, 2 Jan 2003, PGN-ed]
http://www.boston.com/dailynews/002/economy/H_R_Block_employee_accused_of_.shtml

⚡ Half-million people victimized by stolen hard-drives

Monty Solomon <monty@roscom.com>

Thu, 2 Jan 2003 18:05:17 -0500

SSNs and other personal information for a half million military personnel and family members were stolen from hard-drives belonging to Phoenix-based TriWest Healthcare Alliance on 14 Dec 2002. [Source: Associated Press item, \$100K Reward for stolen ID data, 2 Jan 2003; PGN-ed... Coincidentally, DoD is in the process of computerizing medical records of all military personnel. Can they spell Security? Encryption? Identity Theft?]

<http://www.wired.com/news/privacy/0,1848,57045,00.html>

Woman shot by former classmate who stalked her by Internet

Monty Solomon <monty@roscom.com>

Tue, 31 Dec 2002 02:06:01 -0500

A former classmate of Amy Boyer, 20, paid an Internet information broker to track her down, and then shot her on 15 Oct 1999. Since her death, the family has been fighting to protect other potential victims, most recently suing the information broker for negligence and invasion of privacy. [Source: Parents of slain woman want to stop Internet brokers from selling personal information, by Holly Ramer, Associated Press, 30 Dec 2002; PGN-ed]

http://www.boston.com/dailynews/364/nation/Parents_of_slain_woman_want_to:.shtml

✂ Man allegedly stalks ex-girlfriend with help of GPS

<George.Mannes@thestreet.com>

Fri, 3 Jan 2003 11:57:23 -0500

The story starts here on The Smoking Gun (GPS angle appears at bottom of second page of typed complaint):

<http://www.thesmokinggun.com/archive/pseudler1.html>

As far as I can guess (not confirmed) this is the product allegedly used:

<http://www.landairsea.com/Land%20Air%20Sea%20Smart%20Track%20Brochure.pdf>

Now anyone, for better or worse, can be James Bond.

[A 42-year-old Wisconsin man is accused of stalking an ex-girlfriend by

placing a GPS tracking device under the hood of her car. The device

George refers to is called SmartTrack. PGN]

✂ Credit agencies provide information on your relations under DPA

"Tim Storer" <tws@dcs.st-and.ac.uk>

Mon, 30 Dec 2002 12:30:54 -0000

http://www.bbc.co.uk/cgi-perl/whatson/prog_parse.cgi?FILENAME=20021229/20021229_1700_49700_9239_40

[http://www.bbc.co.uk/cgi-perl/whatson/prog_parse.cgi
?FILENAME=20021229/20021229_1700_49700_9239_40](http://www.bbc.co.uk/cgi-perl/whatson/prog_parse.cgi?FILENAME=20021229/20021229_1700_49700_9239_40)

The programme is A Right to Know presented by Michael Crick on BBC Radio 4. He requested information held on him by a credit agency under the Data Protection Act. Interestingly, the company supplied the information -- including the credit history of another member of his family because this is used to assess your own rating. Apparently the agency's policy was to supply the data on other occupants at an address if they shared a surname. The representative of the agency didn't seem overly clear as to whether this procedure had now been corrected. Crick goes on to point out the rather obvious risks...

PGP.COM cannot handle sales to some US residents

"Michel E. Kabay" <mkabay@norwich.edu>
Tue, 31 Dec 2002 14:52:46 -0500

PGP.COM's Web site is programmed so that customers can go through all the forms required to order and pay for a license for PGP -- and then can refuse access to the download after the credit-card has been debited if it cannot do a reverse IP lookup on what it receives as the customer's IP address.

The following message appeared on my screen when I clicked on the download button: "In accordance with current US Export restrictions, PGP

8.0 products

may be downloaded by individuals throughout the world except those in the following countries: Cuba, Libya, Iran, Iraq, North Korea, Sudan, and Syria. If you are in one of these countries, you may not download PGP software."

I was downloading from Vermont using my StarBand account. I tried again after disabling my firewall -- no luck.

The customer service agent was very nice and obviously embarrassed about this situation and admitted that there are no measures in place for dealing with such a technical glitch. She diffidently suggested that I try to download the product again using a different ISP or Internet access point.

I did suggest that the company might deal with such glitches in several ways:

- 1) Check the IP address BEFORE the user fills out all the forms and the credit card gets debited.
- 2) Send the user a CD-ROM to the US address listed in the order.
- 3) Ask the user for strong evidence that they are in fact living in the US: e.g.,
 - a) have the user send a fax from the appropriate US fax machine phone line with a US driver's license showing the same address as the one used in the order;
 - b) ask for other corroborating evidence such as a US address

listing in
university or corporate Web sites.

Of course, I canceled the charge on my card. Someday (not soon), I'll try to download the product from my university access point and -- if the university firewall does not conceal my IP address -- maybe I'll succeed in giving these people my money in return for an upgrade to their product. In the meantime, I'll just continue using my PGP v6.5.8

RISKS of assuming your automated system is perfect: you lose sales.

M. E. Kabay, PhD, CISSP <http://www2.norwich.edu/mkabay/index.htm>

* Associate Professor of Information Assurance
Dept. of Computer Information Systems

* Program Director, MSc in Information Assurance
<http://www3.norwich.edu/msia>

Norwich University, Northfield VT +1.802.479.7937
mkabay@norwich.edu

✶/Trivial/ Risks of Technical Arrogance

"melandrob.searle" <melandrob.searle@actrix.co.nz>
Thu, 2 Jan 2003 16:36:22 +1300

I am just about calmed down after a trying time with a christmas present for a five-year old. The whole sorry episode is of course my fault, I merely needed to read the minimum system requirements more thoroughly and remember

precisely the characteristics of the family machine.

The details :

The game - shall remain nameless to protect somebody.

The stated minimum system:

Win 95 (OK I have XP which should be compatible and Google says the

game was released last year so I assume that the vendors/
game

programmers mean or equivalent)

Pentium 90 MHz or faster (Much faster)

16 MB RAM (More than that)

15 MB Hard Disk (No problem)

Quad-speed CD-ROM (Yeah, yeah)

Stereo sound card (Got a sound card, two speakers ----- Oops
missed

that one)

So, eager five-year old by my side, go through installation.

Fool the

registration screen by lying about the location of Canterbury
and the postal

code (already said the country is Other but the stupid screen
will not

accept four digit post-codes or state/province abbreviations
outside the

US). First technical arrogance. Installation completed
successfully

Locate the shortcut to the game and launch, wait, FATAL error no
stereo

sound game over. Second technical arrogance and this one gets me
steamed up

enough to write.

I have worked on system and product software for nearly eighteen
years and

every year somebody decides that the behaviour under an error
condition can

be specified by the programmers (only the expected normal
behaviour is a

requirement). Handling of errors is ALWAYS a system issue. (My

feelings on
the game are that it is a bit like causing a core meltdown in a
nuclear
facility because the siren doesn't work).

Programmers in their techy way decide that the minimum hardware
is a
critical environmental requirement and nobody told them that the
PC on their
desk may be a bit better specified than the typically
available. Has nobody
heard of graceful degradation ?

✶ Oregon proposing taxing in-state car mileage via GPS

Mike Hogsett <hogsett@csl.sri.com>

Wed, 01 Jan 2003 13:43:55 -0800

<http://news.statesmanjournal.com/article.cfm?i=54184>

Despite "To protect drivers' privacy, using the system to track
cars in
real time would be illegal" the risks seem obvious.

What about travel on private land and/or off-road mileage? Who
pays when
you car is towed? What about the fact that due to inaccuracies
of GPS your
position when stationary will often bounce back and forth
between the
extremes of those inaccuracies?

✶ Re: Total Information Awareness / O Big Brother

Rev. Fredric L. Rice <frice@SkepticTank.ORG>

Fri, 03 Jan 2003 03:28:41 GMT

The last couple of RISKS have touched upon the so-called "Total Information Awareness" plan that various United State law enforcement and intelligence agencies are planning (dare I say "plotting?") to implement.

The issue of false positives when sifting through the mountain of information that's planned to be collected should be a nice waste of time, money, and resources for our government, diverting them from doing real police work by catching real bad guys but if such a plan is implemented and is eventually developed to a minimum of perfection, innocent, lawful people who simply don't want to be identified, it seems to me, can eventually be so identified. Apparently Americans don't have the right to privacy or the right to lawfully disappear in America.

Quite a few years ago someone anonymously sent me a text document titled, "Vanishing Point: How to disappear in America without a trace" which I originally thought was rather paranoid though, with the passage of the euphemistically named "Patriot Act" I'm thinking might not be so paranoid at all. After removing some of the more irresponsible text fragments from it, I posted it to my Web site, where it can be found at <http://www.skepticTank.org/hs/vanish.htm>

One of the suggested items is:

Alter your buying habits. When you throw your old self away, you need to discard as many predictable patterns as possible. One of the most common

mistakes when hiding is maintaining old habits. If you're a smoker, stop. If you don't smoke, start. If you enjoy hot and spicy foods, stop purchasing those items and change to mild foods. If you frequent bars, stop. This may seem an unusual step but you're working toward disappearing, right? Patterns are predictable. Break them.

There is the possibility that in the future people may be identifiable by their purchasing habits. Granted the point-of-sale data collected by computers would need to be immense yet eventually pattern-recognition software may some day be able to provide authorities with perhaps 100 of the best possible "hits" on people matching your known buying habits. When -- if ever -- that becomes a reality, you can be sure you won't know about it until it's shown on cable television. By that time the technology will have been in use for years and you may end up on a list of possible matching a purchase profile.

It seems more and more likely to me that such technology will be upon us thanks to the galloping fascism we're experiencing in America ...

✶ Re: Computer programmer faces U.S. fraud charge ([RISKS-22.44](#))

"Bob Morrell" <bmorrell@wfubmc.edu>
Mon, 30 Dec 2002 18:39:26 -0500

Regarding the attempted manipulation of stock via spreading a

virus in the company, the item noted "He had reportedly been hoping to gain from the resulting stock price drop." This might leave the RISKS digest reader with the impression that the price of the stock did in fact fall as the result of the viral infection, which is not true, according to the NYTimes article, a link to which Mr. Solomon also provided. The article states: "The plan failed when a computer virus that Mr. Duronio personally transmitted to 1,000 of the 1,500 computers used by PaineWebber brokers across the country failed to disrupt work seriously or cause a sharp change in the stock price." It wasn't that the virus was, like most viruses, harmless, or that computers are just not as important as we all think... Apparently backup computers kicked in and minimized any disruption.

Good management of RISKS. Thank you Paine Webber... [And incomplete PGN-ed]

✶ **Re: Surgical tool left in woman's stomach for 4 months ([R-22.44](#))**

John Sullivan <john.sullivan@thermoteknix.co.uk>

Fri, 3 Jan 2003 14:21:50 +0000

Well, the CNN URL has expired and I can't find anything via their search facility, so taking a hint from the URL looked it up directly on reuters.com:

"Why Does This Metal Detector Keep Going Off??"

<http://www.reuters.com/newsArticle.jhtml?>

[type=topNews&storyID=1921184](http://news.google.com/news?hl=en&q=surgical+retractor&btnG=Search+News)

"Several days later the woman had an X-ray [...] It showed a 12-inch-long, 2-inch-wide surgical retractor".

Hmm.

None of "canadian", "surgical" or "retractor" find it even on Reuters, despite those words definitely being in the article, only "x-ray" seems to turn it up. Looking at news.google.com whose search actually works gives more variations: 33cm; 30cm x 5cm; 30cm (11.7in); 11.7in; 11.7in x 5cm; 30cm x 6cm; 30cm (13in) x 6cm (2in); 13in.

<http://news.google.com/news?hl=en&q=surgical+retractor&btnG=Search+News>

You can almost trace the history of unit conversion and rounding errors through the various sources. A RISK various space agencies are painfully aware of. Averaging to get a more accurate figure ;-) gives about 12 inches though.

Ow.

[I had already updated the archive copy, which notes the broken URL, offers

<http://www.hon.ch/News/HSN/510912.html>

instead, which says it was a 33-centimeter retractor. PGN]

✶ Caller ID untrustworthy (was: Why you should read Mitnick's book)

Mathew Lodge <mathew@mathewlodge.com>

Fri, 03 Jan 2003 14:00:30 -0800

> ... So don't trust caller ID to show that the caller is
> someone you know,
> or from your own company. [Don Norman]

I was thinking about this last night when I called American Express to dispute a charge. Normally, after entering your card number, Amex has requires the last four digits of your SSN to "authenticate" you (no risk there, right? :-). This time, a recording said something like "we have verified your home or office phone number" and connected me to a customer service rep who asked no further authorization questions.

Faking caller ID is a lot easier these days because you don't need to buy a DMS-100 (bulky and expensive), learn how to program it (a specialized task with little generally available documentation), and buy the right kind of interconnect to your local telco (the really expensive and time-consuming bit).

Any voice over IP gateway that uses an ISDN PRI interface will allow you to configure any calling number (caller ID) you like, and then signal it to the PSTN via the PRI during call set-up. The ability to control caller ID is necessary to seamlessly integrate VoIP endpoints (e.g. IP Phones) into the PSTN.

A Cisco 3620 would do the job, is 2" high by 19" wide and can be bought on Ebay today for \$849. There is good, free 3620 configuration advice on www.cisco.com. There are likely cheaper alternatives, I just

know setting
caller ID can be done on a 3620.

T1 PRI pricing is dependent on your distance from the central office and whether you have a competitive alternative to your local RBOC, but can cost as little as \$300/month. An E1 PRI will work just as well overseas.

REVIEW: "Protect Your Digital Privacy", Glee Harrah Cady/Pat McGregor

Rob Slade <rslade@sprint.ca>
Thu, 5 Dec 2002 08:17:04 -0800

BKPYDPRV.RVW 20020924

"Protect Your Digital Privacy", Glee Harrah Cady/Pat McGregor, 2002,
0-7897-2604-1, U\$29.99/C\$44.95/UK#21.99
%A Glee Harrah Cady glee@ix.netcom.com
%A Pat McGregor
%C 201 W. 103rd Street, Indianapolis, IN 46290
%D 2002
%G 0-7897-2604-1
%I Macmillan Computer Publishing (MCP)
%O U\$29.99/C\$44.95/UK#21.99 800-858-7674 317-581-3743 info@mcp.com
%O <http://www.amazon.com/exec/obidos/ASIN/0789726041/robsladesinterne>
%P 652 p.
%T "Protect Your Digital Privacy: Survival Skills for the Information Age"

Part one sets the stage. Chapter one gives vague ideas about protecting your privacy in the twenty first century, mostly about e-commerce. A variety of definitions of privacy, from differing

perspectives, are listed in chapter two.

Part two discusses privacy and the individual. From celebrity magazines to publicly available government databases to e-commerce loyalty programs, chapter three discusses who might want to know different types of information about people. Chapter four presents the usual information about kids and the net: the net is potentially dangerous for kids, talk to your kids about their net use, and safe sites. Although there is nothing new here, the material is reasonable and well presented. Email address harvesting and cookies are reviewed in chapter five. Chapter six talks about high speed Internet access, including little content on security or privacy, but an odd bit on malware. There is a similar discussion of cellular phones and technology in chapter seven. Chapter eight examines cell phone location systems, "pay-fobs," face recognition and other miscellaneous technologies.

Part three talks about taking control of your privacy and information. Chapter nine suggests taking an inventory of your personal information (available online) and looks at Web search engines and the inaccuracy of commercial search services. Chapter ten is a mixed bag of security topics, including a little cryptography, something on passwords, and cookies again. Although there are some good tips on protecting online transactions, chapter eleven suffers from a lack of structure. The advice to know where you are and who you are dealing with, for example, is on page 308, but the material on server authentication is

on page 294. Neither location actually demonstrates the ability to verify the certificate, or the "Paypal/Paypal" fraud. Chapter twelve deals with what to do if your information is compromised, but doesn't cover the topic particularly well. There is mention of spam filters, but not the dangers of losing email; there are directions for reporting frauds, but few details on the levels below which the agencies aren't interested; addresses of credit agencies, but little useful information on identity theft.

Part four looks at legal protection. Chapter thirteen is an excellent overview of laws regarding privacy, covering both the United States and a number of other countries. (While the rest of the book is primarily directed at home users, this chapter alone may be worth the price of the volume for security practitioners. I am not aware of any other text that deals with current laws as well.) Advocacy groups are listed in chapter fourteen, with self-regulation programs in fifteen. Electronic voting is examined in chapter sixteen, concentrating on Internet or online voting, although most of the studies cited dealt with other forms of voting technology. Chapter seventeen asks where we are going, and meanders around so much that it is hard to say. There is a vague wrapup in chapter eighteen.

A number of other authors have attempted to provide a book about privacy for the masses. Chris Peterson's attempt (cf. BKILIWMP.RVW) was about privacy, but not really about the net. David Brin's "The Transparent Society" (cf. BKTRASOC.RVW), which gets a mention in the

current work, is fascinating, but doesn't really cover the present situation. "Privacy Defended" (cf. BKPRVDFN.RVW) is only nominally about privacy. Cady and McGregor have managed to stick pretty close to the topic. They present a good deal of useful information, although the book would definitely benefit from an improved framework and a general tightening up of the writing: with a trimming of verbiage and a more focussed thread to the ideas the volume could be lightened by a third or more. However, for those who want some guidance on the topic and don't want the academic classics like "Privacy on the Line" (cf. BKPRIVLN.RVW) or "Technology and Privacy" (cf. BKTCHPRV.RVW), this would be a good choice.

copyright Robert M. Slade, 2002 BKPYPDRV.RVW 20020924
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

<http://victoria.tc.ca/techrev/~rslade> or <http://sun.soci.niu.edu/~rslade>

★ REVIEW: "Privacy Defended", Gary Bahadur/William Chan/Chris Weber

Rob Slade <rslade@sprint.ca>
Mon, 9 Dec 2002 08:18:12 -0800

BKPRVDFN.RVW 20020923

"Privacy Defended", Gary Bahadur/William Chan/Chris Weber, 2002,
0-7897-2605-X, U\$34.99/C\$54.99/UK#25.50

%A Gary Bahadur gary@foundstone.com

%A William Chan william@foundstone.com

%A Chris Weber chris.weber@foundstone.com

%C 201 W. 103rd Street, Indianapolis, IN 46290

%D 2002
%G 0-7897-2605-X
%I Macmillan Computer Publishing (MCP)
%O U\$34.99/C\$54.99/UK#25.50 800-858-7674 info@mcp.com
%O [http://www.amazon.com/exec/obidos/ASIN/078972605X/
robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/078972605X/robsladesinterne)
%P 699 p.
%T "Privacy Defended: Protecting Yourself Online"

The introduction states that this is a privacy book for non-specialists, but the write up seems to deal with computer intrusions or malware rather than privacy issues.

Part one talks about life in the digital age. Chapter one is an unconvincing demonstration of how to obtain personal information online plus more on intrusions and a lengthy outline of the rest of the chapters in the book. There is a slightly unfocused look at privacy laws and related issues in chapter two. Various government, industry, commercial, and other groups and agencies (as well as a few programs) are described in chapter three.

Part two tells us that the enemy is out there. Chapter four points out legal threats to individual privacy that people may not know about, but not in much detail. Illegal threats, such as blackhats, intruders, identity theft, and fraud (as well as those of questionable legality, like spyware) are reviewed in chapter five.

Part three looks at protecting your privacy. Chapter six lists lookup and anonymity tools. Cookies, spyware, some tools, and payment systems are presented in chapter seven. Spam, malware, and PGP are discussed in chapter

eight, along with miscellaneous other topics related to e-mail.

Part four advises on securing your PC. Chapter nine reviews SSL (Secure Sockets Layer) and digital certificates, but because cryptography has not been explained the background discussion is poor. (It is also sometimes erroneous: for most people SSL does *not* authenticate the client.) A collection of random security factors and tools, by operating system, is presented in chapter ten. (The division by operating system is not always clear: tools vary on different versions of Windows, and this is not made clear. There are also a number of errors: IPsec is an Internet protocol and has nothing to do with the Microsoft Windows IP Security Policy.) Screenshots of configuration menus for personal firewalls make up most of chapter eleven. Chapter twelve deals with viruses (poorly), chat (chat systems seem to be almost inherently insecure, so it's hard to understand why), and cryptography (poorly and briefly). Miscellaneous and random network topics are covered in chapter thirteen.

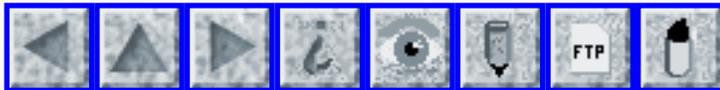
Part five looks at other devices, in a single chapter, fourteen, covering various gadgets, threats, and protections--not necessarily for those threats.

Part six says what to do if your privacy is compromised. Chapter fifteen mentions kids, mostly rehashing previous material and adding content restriction. Intrusion detection and a review of other tools from prior chapters finishes out in sixteen.

This book is not really about privacy, it is yet another attempt at a general security guide. "Protect Your Digital Privacy" (cf. BKPYPDRV.RVW) sticks much closer to the privacy topic. "Inside Internet Security" (cf. BKININSC.RVW) and even "Access Denied" (cf. BKACCDEN.RVW) are better at covering general security for non-professionals.

copyright Robert M. Slade, 2002 BKPRVDFN.RVW 20020923
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

<http://victoria.tc.ca/techrev/~rslade> or <http://sun.soci.niu.edu/~rslade>



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

[ACM](#) Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 47

Monday 6 January 2003

Contents

- [Bruce Schneier: Counterattack and vigilantism](#)
[Monty Solomon](#)
- [Risks of diverse identification documents](#)
[Markus Kuhn](#)
- [Over 160,000 join Massachusetts list to block telemarketers](#)
[Monty Solomon](#)
- [Automakers block crash data-recorder standards](#)
[Monty Solomon](#)
- [Re: O Big Brother, where are thou?](#)
[Jerrold Leichter](#)
- [Re: Caller ID untrustworthy](#)
[Danny Burstein](#)
[Jerrold Leichter](#)
- [REVIEW: "Minimizing Enterprise Risk", Corinne Gregory](#)
[Rob Slade](#)
- [REVIEW: "Enterprise Information Security", Peter Gregory](#)
[Rob Slade](#)
- [REVIEW: "Enterprise Security", David Leon Clark](#)
[Rob Slade](#)
- [Info on RISKS \(\[comp.risks\]\(#\)\)](#)

✶ Bruce Schneier: Counterattack and vigilantism

Monty Solomon <monty@roscom.com>

Mon, 6 Jan 2003 08:38:53 -0500

Excerpt from

CRYPTO-GRAM, December 15, 2002

by Bruce Schneier

Counterattack

This must be an idea whose time has come, because I'm seeing it talked about everywhere. The entertainment industry floated a bill that would give it the ability to break into other people's computers if they are suspected of copyright violation. Several articles have been written on the notion of automated law enforcement, where both governments and private companies use computers to automatically find and target suspected criminals. And finally, Tim Mullen and other security researchers start talking about "strike back," where the victim of a computer assault automatically attacks back at the perpetrator.

The common theme here is vigilantism: citizens and companies taking the law into their own hands and going after their assailants. Viscerally, it's an appealing idea. But it's a horrible one, and one that society after society has eschewed. ...

<http://www.counterpane.com/crypto-gram-0212.html#1>

✦ Risks of diverse identification documents

Markus Kuhn <Markus.Kuhn@cl.cam.ac.uk>

Sun, 05 Jan 2003 01:09:40 +0000

The Home Office is currently running a consultation exercise on the introduction of an identity infrastructure for Britain. This would consist of a biometric database with basic records of the entire population. Anyone in the database would be able to get an identity card, which would essentially enable the holder to grant easily read access to his or her record to any peer who needs some form of assurance about one's identity. Details on the consultation are on

<http://www.homeoffice.gov.uk/dob/ecu.htm>

The system proposed is nothing unusual and quite similar to what most European and many Asian countries have used successfully for several decades.

Such identity infrastructures are generally widely accepted in these countries, where most people consider them today to be a desirable and effective protection against what has become known in some countries that still lack them as "identity theft".

Nevertheless, there is fierce opposition to the proposals from various British privacy advocacy groups. Similar discussions can be observed at the moment in the US and Japan.

While much of the opposition is of a somewhat religious/tinfoil-hat nature and therefore difficult to address, some of it has been voiced by notable computer-security experts and therefore deserves some serious response.

The probably most commonly recurring theme is that the introduction of a national identity card would lead to over-reliance on a single document. The need to corrupt only the issuing procedures of a single mechanism -- so the often expressed concern -- would ultimately make identity theft easier rather than harder. This is probably based on the implicit assumption that independent identity systems perform independent checks with statistically independent failure probabilities. Therefore their security should increase exponentially with the number of verification systems and more would be better.

Defense-in-depth and its use of multiple diverse security mechanisms is in general a feature of sound security engineering. However, applying this general idea in the context of government infrastructures against identity theft this way is in my opinion horribly wrong and naive for a number of reasons, which I'd like to address very briefly.

The most obvious problem is that the UK's present alternative -- identification based on multiple documents and issuing procedures -- adds very little as none of the currently widely available documents is protected by controls of desirable strength. This is just illustrated again by recent

media demonstrations on how easily it is to abuse UK birth certificates:

http://news.bbc.co.uk/1/hi/programmes/kenyon_confronts/2625395.stm

In practice, anyone wishing to verify an identity gets only the *minimal* protection of all the ID schemes in common use, because as soon as you break one of them, you can quite easily proliferate your fake identity into several other systems. Get a fake UK birth certificate (fairly easy) and apply with it for a fake UK drivers license (therefore also not much more difficult), use both to get a fake UK passport and all three to comfortably get fake account access, education degrees, travel documents, security clearances, etc. etc. Most of the existing systems depend on each other, which leads easily to circular verification (A thinks B knows I and B thinks A knows I). They all lack the somewhat more expensive direct checks of non-document evidence that for example a properly protected distributed add-only database of the biometric long-term history of those registered could support economically and effectively.

Multiple documents? Unfortunately, the world of fake ID documents currently works more like "Buy one, get three more free!" The number of systems doesn't count much after all.

But this is not the only reason why it is so crucial to have at least one identification scheme that is seriously difficult to break, while having more than one of these is unlikely to be worth the cost and

hassle.

There is first of all also the problem that within a single infrastructure, it is far easier for those in charge of its integrity to verify and ensure that the overall policies such as the separation of duties for critical checks really leads to checks that are independent by design, and not by chance.

Another reason is that the costs for the training/equipment/time/etc. necessary for the adequate verification of security documents increases at least linearly with the number of different document types accepted. And the risk of fraudsters finding by brute-force search one accepted type of identification for which a particular verifier is not well prepared to recognize comparatively simple fakes increases even exponentially with the overall number of different identification forms accepted.

Hence I am not surprised by the desire in the UK government to finally also offer its tax payers one single simple cheap properly engineered and run identity infrastructure. It is needed to replace all the existing often ridiculously weak alternatives (including old birth certificates, old driving licenses, magstripe-cards, knowing mother's maiden name or showing a laser-printed utility bill) that are all currently used by especially the UK financial industry as acceptable means for gaining access to critical personal information and property.

Perhaps the discussion should first of all be driven by

comparing actual practical identity-theft versus privacy-violation statistics in countries with and without proper government-provided identification infrastructures, instead of naively applying generic security recipes such as more-mechanisms-are-better to an application area with far more specific properties.

Markus Kuhn, Computer Lab, Univ of Cambridge, GB
<http://www.cl.cam.ac.uk/~mgk25/>

Over 160,000 join Massachusetts list to block telemarketers

Monty Solomon <monty@roscom.com>
Fri, 3 Jan 2003 19:38:03 -0500

The brand-new Massachusetts anti-telemarketing Do-Not-Call Registry had 20,000 people enroll even before it opened officially on New Year's Day, and then 140,000 more in its first two days of official existence. State officials anticipate that one-third of Massachusetts' 3 million residential customers will sign up in the first month.

[Sources: Bruce Mohl, *The Boston Globe*, 3 Jan 2003; and Signup begun to ward off telemarketers, Associated Press, 1 Jan 2003' PGN-ed]

http://www.boston.com/dailyglobe2/003/business/Over_140_000_join_list_to_block_telemarketers+.shtml
http://www.boston.com/dailyglobe2/001/metro/Signup_began_to_ward_off_telemarketers+.shtml

✶ Automakers block crash data-recorder standards

Monty Solomon <monty@roscom.com>

Mon, 30 Dec 2002 00:16:03 -0500

Highway safety could be vastly improved if black boxes that record information about car crashes were standardized, experts say, but they contend that vehement objections from the automobile industry are thwarting efforts to set a standard. About 25 million late-model cars and trucks, most built by General Motors and Ford, carry the boxes, which record crash information including how fast a vehicle was moving, whether the seat belts were buckled and how big a jolt the occupants suffered at impact. ...
[Source: Matthew L. Wald, *The New York Times*, 29 Dec 2002; PGN-ed]

<http://www.nytimes.com/2002/12/29/national/29CRAS.html>

✶ Re: O Big Brother, where are thou? (Nilges, [RISKS-22.45](#))

Jerrold Leichter <leichter@lrw.com>

Sat, 4 Jan 2003 10:53:08 -0500 (EST)

spinoza1111@yahoo.com (Edward G. Nilges) notes that TIA -- which he doesn't like -- will apparently be based on the commercial Groove software product and notes that those TIA is targeting will thus have access to the same software and can modify what they do to avoid being spotted by it. Preventing this, he claims, is equivalent to the Halting

Problem. The politicians, as usual, are ignoring "the facts" because they are inconvenient.

Nonsense. The Halting Problem has nothing whatsoever to do with the use of off-the-shelf software, with TIA, or with anything I've seen proposed. I have many doubts about TIA myself, but the last thing we need is pseudo-science -- scientific words used inappropriately to give an imprimatur of "objective, scientific fact" to an unrelated argument. (See the use of "energy" in any ad for crystals or other new-age, hmm, product.)

Why does the Halting Problem have nothing to do with this? Does Mr. Nilges seriously believe that Groove, whatever it might do, comes out of the box configured to search for terrorist activity? Let's get real here: Any product of this sort is a framework; you tune it to look for what you think is of interest.

Let's apply Mr. Nilges's argument to a simpler setting. I propose to scan mail messages for the use of various terms of interest using my secret, proprietary perg program. You wish to send messages that won't trip my detector. Does it help you in your attack if you find out that perg is actually grep, which you have a copy of? What you need to know is what keywords I'm looking for -- not *how* I'm searching for them. Sure, maybe knowing that I'm using regular expressions will help you in theory, but unless you are willing to use messages of unbounded length, there actually isn't any difference between regular languages and even

unrestricted
languages.

Now, no one would propose using grep, or any such simple-minded search, for this kind of thing today -- whatever jokes Mr. Nilges makes about "hackerz". If we start at the lexical level, the existence, for many years now, of text-to-speech converters with human-level performance means that alternate spellings that have recognizable pronunciations can be readily recognized. But a few minutes with even a program that's way behind the state of the art -- the grammar checker in Word -- shows that programs these days do a reasonable job of recognizing fairly deep syntactic and semantic aspects of natural language. Or try some of the translators out there - they can produce some hilarious results, but look at how often they get the basics right. If what you are looking for is a system that stands a good chance of picking up "suspect" text, and you are willing to accept false positives -- the technology is probably there.

Beyond all this, like the silly MIT paper about random vs. targeted searching at airports, Mr. Nilges ignores the fact that, while any search system will probably end up looking at many "incidental" aspects of (say) terrorism (e.g., buying one-way tickets), some are fundamental (if you want to produce a bomb, you need explosives, and while there are a variety of explosives around, but not an unlimited variety), and some are incidental but difficult to change (you *could* receive terrorist training anywhere, but in practice there are only so many places in the world where

there are training camps; visiting those areas is a pretty good indicator). And even the "pure incidentals" can be valuable as long as they are secret.

There are many legitimate complaints to be made about TIA on social and political grounds. There are also practical issues of implementability, though many have more to do with scaling than anything else -- data mining, difficult as it is to justify on theoretical grounds, seems to work well enough that many businesses are spending -- and saving -- questions to doublecheck.

⚡ Re: Caller ID untrustworthy (Lodge, [RISKS-22.46](#))

danny burstein <dannyb@panix.com>

[DUE TO AN EDITING ERROR, THE ABOVE HEADERS FOR THE FOLLOWING ITEM

SOMEHOW GOT LOST. I BELIEVE THE TEXT BELOW IS INTACT.]

On the other hand, if you call from your work number then the service rep will ask quite a few more questions.

Now the key thing here is, as the original poster pointed out, the validity and accuracy of the displayed phone number.

And yes, standard "caller id" (more officially known as "calling party number" or CPN) can be spoofed. Or, for that matter, be inaccurate. Or

wrong. Sometimes maliciously, sometimes for good reason.

A legitimate purpose, for example, would be at a hospital. When a nurse calls out from the fourth floor intensive care unit the CPN might be sent over as the main hospital number. On the other hand, a telemarketer may have other reasons for making you think a call is local...

However, when you call a 1-800/888/877/866 (and soon 855) toll-free "area code" [a] number such as in this case, the phone number showing up on the display is NOT the CPN, but rather is courtesy of Automatic Number Identification (ANI). This number is generated and sent across by the telco, NOT by your equipment, and is much, much, harder to falsify.

(ANI is used internally by the telcos and the long distance carriers and similarly connected groups for, among other things, billing purposes.) [b]

While these two numbers (CPN and ANI) are often the same, and in the case of residential users and small businesses are almost always identical, this is not always the case.

But again, the key point for RISKS is that spoofing ANI takes a lot more knowledge, equipment, and access, than commonly available.

[a] 800/888/877/866 "area codes" are technically called "service access codes" since they don't have geographic distinctions. In the Old Days the first three digits of the phone number following the 800 did provide destination routing -- for example, 800-225-.... was the Boston area, but

that hasn't been the case for a long, long, time.

[b] since the company you're calling pays the charge, they have the right to get a full detailed listing of the phone numbers reaching out to them. In the case of AMEX, etc., this is a realtime display on the service rep's screen -- which will also pull up your account info with them. The local tow-truck company, on the other hand, may simply get it as a printout in the monthly bill.

✶ Re: Caller ID untrustworthy (Lodge, [RISKS-22.46](#))

Jerrold Leichter <leichter@lrw.com>
Sat, 4 Jan 2003 09:43:22 -0500 (EST)

[Much of the content of Danny's message (above) was also noted in detail

by Jerrold Leichter. In order to avoid duplication, I have omitted part

of Jerry's message, but included his last paragraphs, where CLID refers to

Calling Line ID, also known as Calling Number ID, and incorrectly as

Caller ID. Apologies if I left out something nonduplicative. PGN]

By its nature, ANI must be difficult to forge. (Also by its nature, it may not point to a number that would make sense to the average person: It identifies the line that should be billed, which may or may not correspond to a dialable telephone number.) Telephone companies want to be paid, and

won't let someone into a position where they can specify ANI unless they are sure they will be good for the charges. PBX users can specify CLID, but ANI is set at "the other end of the link". Does this mean ANI can't be faked? Certainly not, but the massive fraud *against them* that such fakery would allow would certainly drive the Telcos to fight it vigorously.

Just to complete the picture: *Receiving* ANI isn't cheap. Commercial-scale 800 services from the major Telcos deliver true ANI. Consumer 800 number services have no way to deliver ANI, since consumers have to direct way to receive it. But there's an intermediate level: Some of the cut-rate 800 providers sell services that deliver what looks like ANI information, but is actually derived from CLID (since that way they don't have to pay to get the ANI from the Telco they connect to). Obviously, you as a customer have no way of knowing if the company you called is fooling itself by buying cheap 800 service -- but on the list of things to worry about, that certainly can't be all *that* high. -- Jerry

🔥 REVIEW: "Minimizing Enterprise Risk", Corinne Gregory

Rob Slade <rslade@sprint.ca>
Mon, 6 Jan 2003 08:09:27 -0800

BKMIENRI.RVW 20020916

"Minimizing Enterprise Risk", Corinne Gregory, 2003, 0-273-66158-2,

UK#156.99/C\$319.99

%A Corinne Gregory corinne.gregory@hartgregorygroup.com

%C London, UK

%D 2003

%G 0-273-66158-2

%I Prentice Hall/Financial Times

%O UK#156.99/C\$319.99 +1-201-236-7139 fax: +1-201-236-7131

%O [http://www.amazon.com/exec/obidos/ASIN/0273661582/
robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/0273661582/robsladesinterne)

%P 120 p.

%T "Minimizing Enterprise Risk: A practical guide to risk and
continuity"

Chapter one defines four types of risks--and immediately contradicts itself with tables of other types of risks. The basic point seems to be that risks exist. Chapter two looks at the new product development process and reputation management (after all, one type of risk is bad publicity). There is a look at risk mitigation, but not risk acceptance or avoidance, a cost/benefit analysis that is not very detailed, and a contrived use of the "9/11" World Trade Center disaster (but no mention of the brokerage firm that survived) that undercuts the ultimate message about having a disaster plan. Enterprise continuity, in chapter three, has, like other chapters, good ideas mixed in with a random collection of topics from business continuity planning, disaster recovery, incident response, contingency planning, and other areas. Business impact analysis is proposed as a justification for planning, in chapter four, although it should be part of risk analysis itself. Otherwise this material is pretty basic; get a committee, list the risks, think of what to do about them; the type of thing

you would see in any decent article on risk management. Chapter five states that Internet use is risky, and has a (short) list of some precautions.

Anyone who thinks that they understand risk management or business continuity planning from reading this book is seriously misled, and possibly a liability to the company.

copyright Robert M. Slade, 2002 BKMIENRI.RVW 20020916
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

<http://victoria.tc.ca/techrev/~rslade> or <http://sun.soci.niu.edu/~rslade>

★ REVIEW: "Enterprise Information Security", Peter Gregory

Rob Slade <rslade@sprint.ca>
Fri, 3 Jan 2003 08:09:33 -0800

BKENINSE.RVW 20020916

"Enterprise Information Security", Peter Gregory, 2003, 0-273-66157-4,

C\$19.99/UK#156.99

%A Peter Gregory peter.gregory@hartgregorygroup.com

%C London, UK

%D 2003

%G 0-273-66157-4

%I Prentice Hall/Financial Times

%O C\$19.99/UK#156.99 +1-201-236-7139 fax: +1-201-236-7131

%O <http://www.amazon.com/exec/obidos/ASIN/0273661574/>

[robsladesinterne](#)

%P 145 p.

%T "Enterprise Information Security: Information security for non-technical decision makers"

The executive summary states that this book is intended to present information security to executives. The introduction certainly shows that it isn't intended for technical people, who would ask what the difference was between access over the Internet and remote access, or a network using TCP/IP and the Internet.

Chapter one asserts that the events of September 11, 2001 woke executives up to the importance of security. (Yeah, right.) However, there is a good analysis of the reasons that the Code Red/Nimda worm was successful. The definition of a threat, in chapter two, is pretty bad, and the definitions of various types of malicious software are really bad. The section on hacking lists a variety of attacks (heavy on social engineering), the "hacker profiles" concentrate on system exploits, there is a random list of security problems, and then an surprisingly good definition of vulnerability. Authentication and authorization are reasonably handled, but confused with extraneous details in chapter three. Access control is equated with firewalls, and the discussion of cryptography is all right but full of minor errors. (RC 2 and RC 4 have been compromised, Skipjack has been released for limited review, a digital signature does need a key but not necessarily an additional password, the loss of a key is not sufficient to repudiate a digital signature, and the ping-of-death does not compromise integrity.) The material on antivirus protection refers only to scanning, and the material on audit deals only with logs. Chapter four is

supposed to be about policies, but actually concentrates on procedures, containing random thoughts and many gaps. People are the weak link in security, we are told in chapter five, and, as with other sections it uses non-standard terms in the discussion. More haphazard thoughts are in chapter six, while chapter seven has a poor definition of privacy and a grab bag of topics. In chapter eight a casual list of topics seem to be indiscriminately assigned to the standard important/urgent quadrant chart.

OK, this is not intended for professionals; it is intended for managers. But, even if we give full reign to the usual jokes -- those who can't, do; those who are incapable of mastering anything, go into management -- it's still bad form to deliberately mislead them this way.

copyright Robert M. Slade, 2002 BKENINSE.RVW 20020916
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

<http://victoria.tc.ca/techrev/~rslade> or <http://sun.soci.niu.edu/~rslade>

✶ REVIEW: "Enterprise Security", David Leon Clark

Rob Slade <rslade@sprint.ca>
Thu, 2 Jan 2003 08:22:00 -0800

BKESTMDG.RVW 20020916

"Enterprise Security", David Leon Clark, 2003, 0-201-71972-X,
U\$39.99/C\$62.99

%A David Leon Clark
%C P.O. Box 520, 26 Prince Andrew Place, Don Mills, Ontario
M3C 2T8
%D 2003
%G 0-201-71972-X
%I Addison-Wesley Publishing Co.
%O U\$39.99/C\$62.99 416-447-5101 fax: 416-443-0948
%O [http://www.amazon.com/exec/obidos/ASIN/020171972X/
robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/020171972X/robsladesinterne)
%P 264 p.
%T "Enterprise Security: The Manager's Defense Guide"

The preface is heavy on buzzwords (and a few spelling errors) with little attention paid to concepts and structure. Part one would like us to think of the forging of a new economy. Chapter one asks "what is e-business," and, with a little re-interpretation of history (the Internet had been in existence for twenty two years and had five million users, a significant number private and commercial, before it "became available to the public" according to this book) and ignoring of inconvenient facts (the hyperinflation of dot com IPO stocks is stated to prove the success of e-business just before we are told that the dot com failure was inevitable because of stock hyperinflation) tells us that e-business uses the net and makes money. Some security jargon is introduced in chapter two. A confused recycling of trade press myths about blackhats, in chapter three, seems to state that these are the only malicious opponents of e-business: there is no mention of insider attacks.

Part two looks at protecting information assets in an open society. Chapter four demonstrates an amazingly consistent failure to understand the

technologies supposedly being explained: a De-Militarized Zone (DMZ) is, by definition, not abandoned outside the firewall, and Simple Key Management for IP (SKIP) is not a virtual private network (VPN) product. There are more buzzwords, miscellaneous security concerns, and more mistakes (ActiveX is **not** multi-environment) in chapter five.

Part three talks about waging war for control of cyberspace. Chapter six looks at attacks by syntax, and demonstrates more TCP/IP errors. (Packet filtering is not exactly built into IP: the ability to handle a packet based on destination is central to the idea of networking. The ping-of-death has nothing to do with fragmentation offsets since it is a single packet, and it is not too small, but too large.) There is a confusion of attack scripts and script viruses (and cookies, too, for good measure) in chapter seven. Countermeasures and attack prevention, in chapter eight, actually looks (tersely) at incident response. The material isn't too bad, but has very little detail. Having talked about DDoS (Distributed Denial of Service) in chapter six, the attack now gets more pages, but little more detail. Chapter ten is a grab bag of random safeguards and countermeasures, as is eleven.

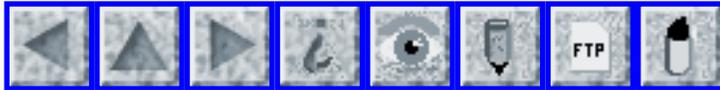
Part four deals with active defense mechanisms and risk management. Chapter twelve, entitled vulnerability management, suggests collecting alerts. Given what we've seen so far, it is strange that chapter thirteen **does** address the nominal subject of risk management, albeit not very

well.

This confused collection of random concepts adds nothing of value to the security literature.

copyright Robert M. Slade, 2002 BKESTMDG.RVW 20020916
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

<http://victoria.tc.ca/techrev/~rslade> or <http://sun.soci.niu.edu/~rslade>



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

[ACM](#) Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 48

Thursday 9 January 2003

Contents

- ['DVD Jon' acquitted by Norwegian court](#)
[NewsScan](#)
- [Supreme Court backs off on DVD descrambling code](#)
[NewsScan](#)
- [Edge conditions and date-rollover bugs](#)
[identity withheld by request](#)
- [Turing Tests for spam](#)
[Chris Leeson](#)
- [S*X.COM ruling could open floodgates on registry lawsuits](#)
[NewsScan](#)
- [Lost header in text of RISK-22.47](#)
[PGN](#)
- [Re: Man allegedly stalks ex-girlfriend with help of GPS](#)
[Alpha Lau](#)
- [Wrong CLID woes](#)
[Richard Snider](#)
- [Re: /Trivial/ Risks of Technical Arrogance](#)
[Bill Bumgarner](#)
- [Re: O Big Brother, where are thou?](#)
[David Martin](#)

[Edward Nilges](#)

● [TIA: Groove is simply a collaboration tool](#)

[Stever Robbins](#)

● [Re: TIA, surveillance, and Tolkien](#)

[Noah Shachtman via Monty Solomon](#)

● [REVIEW: "Building Linux Virtual Private Networks", Kolesnikov/Hatch](#)

[Rob Slade](#)

● [REVIEW: "Know Your Enemy", Honeynet Project](#)

[Rob Slade](#)

● [Info on RISKS \(comp.risks\)](#)

✶ 'DVD Jon' acquitted by Norwegian court

"NewsScan" <newsscan@newsscan.com>

Tue, 07 Jan 2003 08:58:28 -0700

Jon Lech Johansen (also known as DVD Jon), who was accused of illegally developing and distributing the DeCSS program for breaking the digital copy-protection mechanism on DVDs, has been acquitted in a Norwegian court. The rationale for the judge's decision was that the software could be used for legal purposes as well as illegal ones. "If a person's motive is to solely encourage or solicit illegal actions, then it would be illegal to distribute it" -- but the court made the judgment that Johansen was not motivated in that way. [*PC World*, 7 Jan 2003, NewsScan Daily, 7 Jan 2003]

<http://www.pcworld.com/news/article/0,aid,108462,00.asp>

⚡ Supreme Court backs off on DVD descrambling code

"NewsScan" <newsscan@newsscan.com>

Mon, 06 Jan 2003 09:21:41 -0700

The U.S. Supreme Court has rescinded an emergency stay barring defendant Matthew Pavlovich from distributing DeCSS, a software utility that descrambles the digital lock on most DVDs to prevent copying them. Pavlovich is now free to distribute the code, but could be sued again if he decides to do so. "The entertainment companies need to stop pretending that DeCSS is a secret," says Cindy Cohn, legal director for the Electronic Frontier Foundation, which is assisting Pavlovich. "Justice O'Connor correctly saw that there was no need for emergency relief to keep DeCSS a secret. It doesn't pass the giggle test." The rescission is just the latest twist in a case that has been winding its way through the courts since 1999, when the DVD Copy Control Association -- a coalition of movie studios and consumer electronics makers -- filed a lawsuit against scores of people, alleging violations of California's trade secret laws. [CNet News.com, 3 Jan 2003; NewsScan Daily, 6 Jan 2003]
http://news.com.com/2100-1023-979197.html?tag=fd_top

⚡ Edge conditions and date-rollover bugs

<[identity withheld by request]>

Mon, 06 Jan 2003 11:49:16 -0500

An acquaintance found himself puttering around late New Year's Eve with an allegedly general-purpose and high-quality date/time library he'd written. He was using it to count down the seconds until midnight, as programmers are wont to do. The witching hour, however, provided a rather dramatically convincing demonstration that the code in question is **not** quite perfect yet. The countdown showed:

```
2002-12-31 23:59:56.61
2002-12-31 23:59:57.52
2002-12-31 23:59:58.45
dateexpr: newtime.c:618: normalize:
  Assertion `t2.subsec >= 0 && t2.subsec < 1000000' failed.
Aborted (core dumped)
2003-01-01 00:00:00.26
2003-01-01 00:00:01.17
2003-01-01 00:00:02.08
```

(There's some comfort, I suppose, in the fact that the core dump resulted from an assertion failure, as opposed to a wholly unexpected bug...)



✶ Turing Tests for spam

Chris Leeson <CHRIS.LEESON@london.sema.slb.com>
Thu, 09 Jan 2003 10:34:36 +0000

In an attempt to prevent spammers from using "robots" to sign up for multiple free email accounts, companies using Web-based email systems are using "Captchas" (Completely Automated Public Turing tests to tell Computers

and Humans Apart).

Roughly translated, a pass phrase is generated as an image, and then noise is added to the image. The user is then required to type the pass phrase in. The idea is that a human will be able to do this, but a "robot" will not.

The method is not foolproof - some programs can read the pass phrase (admittedly slowly) and some spammers simply redirect the pass phrase to a human.

The problem for legitimate users is that the image may be difficult to read if the user has impaired vision (or worse, is completely blind). Quoting from the article:

"If this new way of presenting password information prevents visually impaired people from using a service then we have a serious problem on our hands," said Julie Howell, campaigns officer at the Royal National Institute for the Blind in the UK. She said legislation in the Britain and US demands that companies make Web sites accessible to people with disabilities. "Security and accessibility must co-exist, not conflict," she said.

The article notes that work is now taking place on sound-based "Captchas". Sadly, this will only shift the problem to people with hearing difficulties.

[Source: BBC News Web site]

<http://news.bbc.co.uk/1/hi/technology/2635855.stm>

✶ S*X.COM ruling could open floodgates on registry lawsuits

"NewsScan" <newsscan@newsscan.com>

Mon, 06 Jan 2003 09:21:41 -0700

A federal appeals court has asked California's Supreme Court to rule on whether Network Solutions Inc., the largest U.S. domain registry, must face a multimillion-dollar damage claim from the rightful owner of the s*x.com domain name. The ruling could lead to a flood of lawsuits against domain registries, particularly NSI, from hundreds of people who claim their domain names were also stolen. The current case stems from a lawsuit filed in 1998 by Gary Kremen who registered the s*x.com name with NSI in 1994. In October 1995, NSI received a letter purportedly from Kremen asking that the name be reregistered to a company headed by Stephen Cohen. NSI complied without attempting to verify the validity of the request, and then refused to undo the transfer when alerted to the fraud. Meanwhile Cohen, who was using the domain name for a lucrative porn business, fled the country before Kremen's lawsuit against him went to trial in 2001. Kremen, who is now using s*x.com for his own porn business, was awarded \$65 million in damages from Cohen for fraud (which he'll probably never collect) and is now requesting an additional \$30 million from NSI for allowing the fraudulent transfer. [*San Francisco Chronicle*, 4 Jan 2003; NewsScan Daily, 6 Jan 2003]

<http://shorl.com/bigrifretomebro>

✶ **Lost header in text of [RISKS-22.47](#)**

"Peter G. Neumann" <neumann@csl.sri.com>

Tue, 7 Jan 2003 9:20:11 PST

My apologies for the error in [RISKS-22.47](#) that seemed to run two unrelated contributions together. The header for Danny Burstein's contribution noted in the CONTENTS of the issue and in the second item by Jerry Leichter was inadvertently omitted. It has been corrected in the official archives, ftp.sri.com at SRI, and risks.org -- which indirections to Lindsay Marshall's catless site at Newcastle. PGN

✶ **Re: Man allegedly stalks ex-girlfriend with help of GPS**

Alpha Lau <avlxyz@yahoo.com>

Sun, 5 Jan 2003 21:34:20 -0800 (PST)

I am a bit curious as to how the GPS SmartTrack unit could get line-of-sight to the GPS satellites while under the metallic hood of the car, which should, unless I am mistaken, block GPS transmissions?

Is it possible that the SmartTrack unit used cellular networking instead? It should be possible if you know the locations of all the cellular

network
base stations. You could determine the strength of each signal
and thus
triangulate the position. Cell phones do this all the time as it
tries to to
hand-off to a neighboring cell.

[Perhaps an oversimplification in the reporting. PGN]

⚡ Wrong CLID woes

Richard Snider <risks@sounds.com>

Tue, 7 Jan 2003 13:32:20 -0500

A few years ago my family moved to a new home and with the new
home we were
assigned a new phone number. After a few months, we began to
get messages
on our answering machine of the type:
"...why did you call me and hang up"
"...who is this"
"...please stop calling us"
and other more strongly worded versions. Since we were never
home at the
time these came in, I assumed that some neighbor with a similar
cordless
phone to ours was "borrowing" our line. This proved to be not
the case and I
wondered what might be happening until finally a person called
to complain
and was actually able to talk to me.

They called and asked for Mr. Med-Deea, I advised them that
there was no-one
present with that name. They told me that someone just called
from my
number so they must be present. I asked them to spell the
name...M-E-D-I-A,
you know Mr. Med-Deea.

Now we were getting somewhere. This was sounding like some fax-spam type company that either intentionally or by mistake programmed their equipment incorrectly. I attempted to pacify the ever-more-irritated lady by offering the above technical explanation. No, she said its my number showing on her box, so it must have been someone at my house that phoned her. Then I told her I would prove it to her. I will phone her myself and so I did. She instantly claimed I was wrong because the same number was showing on her phone. I asked her to look at the name....Oh..it was different. She was happier and I was happier.

I tracked down the previous owner of the phone number, and despite being quite wary of me, seemed to know nothing about telcom, fax marketing, or phones in general, so I ruled out that someone had left the number in some peice of hardware and forgot to change it.

Ultimately, there was not much I could do, although I did not try I assumed that the phone company would not be particularly helpful in this regard. If the calls were originating Intra-Lata, there might be some accounting records for them, but I doubt that anyone could have been convinced to check it out.

Eventually, the calls stopped and we have not had one for over a year now. Either the marketer went bust, or fixed their hardware.

There are many RISKS here, the most important one is that people who do not

understand the technology will tend to not accept explanations that differ from their own.

Re: /Trivial/ Risks of Technical Arrogance ([RISKS-22.46](#))

Bill Bumgarner <bbum@codefab.com>

Sat, 4 Jan 2003 15:24:00 -0500

While this is certainly unacceptable behavior on the part of the application in question and such behavior-- failing gracelessly at the merest hint of something erroneous-- is common to both \$10 kiddie games and \$5,500 studio tools (and everything in between), blaming it on the programmers-- on technical arrogance on their part-- is both misguided and counterproductive.

The real problem lies in how the average software package, Web site, custom development solution, or embedded system is developed.

Typically, the client / product manager / producer / art department / creative crew create a set of story boards / screens / photoshop images / line art on napkins / diagrams that represent the user experience with a hint of what the logic behind it may be required. It is rare that these "blueprints" include anything more than a hint as to what to do when something goes wrong.

As such, handling exceptional situations is largely an afterthought. The

developers may slap something in, but it isn't on their schedule and it is typically done at the last minute under a serious time crunch.

It isn't up to the developer to specify the requirements of a system. As you indicate, their system is not the average and it is extremely unlikely that the average developer will be familiar with what an average system in the target market may be equipped with.

The product manager / client / producer / marketing should have determined the minimum requirements and specified that to the developer. Furthermore, the 'blue prints' should have contained information as to how to handle exceptional situations-- how to fail gracefully.

Most importantly, both time and budget should have been allocated to develop the error handling features properly and to test the software in conditions where it would fail.

In other words: Don't blame the messenger.... and don't blame the soldiers for failing to take a hill when the generals send them into battle with incomplete information.

✶ Re: O Big Brother, where are thou? ([RISKS-22.44-47](#))

"David Martin" <dm@cs.uml.edu>
Wed, 8 Jan 2003 17:37:31 -0500

Conspicuously overlooked in the discussion about Total

Information Awareness

is the lack of any means for the US government to *obtain* the terabytes or whatever it's supposed to sift through. When I asked the deputy director of TIA about this last year, he acknowledged that they would be relying on publicly available and voluntarily supplied data for TIA -- as is typically the case in the construction of prototypes. The story routinely presented in the media is that the government is just doing this to us, and the only hurdles to widespread deployment are purely technical ones. But it seems clear to me that Congress and the courts would have something to say about compelling private businesses to routinely submit their transactional data for government inspection.

David Martin, Computer Science, UMass Lowell <http://www.cs.uml.edu/~dm>

✶ Re: O Big Brother, where are thou? (Leichter, [RISKS-22.47](#))

Edward Nilges <spinoza1111@yahoo.com>

Tue, 7 Jan 2003 14:55:47 -0800 (PST)

Turing limits, like it or not, play a part in the actual application of software; the field would not exist without these limits, since absent the Halting problem automatic methods would have been used, long ago, to debug software. They apply a fortiori to man/machine systems insofar as the human members follow procedures.

>... Does Mr. Nilges seriously believe that Groove, whatever it might do,
> comes out of the box configured to search for terrorist activity? ...

By announcing the use of Groove, the administration has done the bad guy's work for them. In terms of your example, we have sent them a letter saying "perg is grep." This indicates a fundamental lack of seriousness, and that the real purpose of the TIA program is a pork barrel for Bush's friends in the depressed data base industry. It's as if the British could buy the Enigma in Sweden, rather than capturing it!

>Now, no one would propose using grep, or any such simple-minded search, for
>this kind of thing today [...]

This view is based on a mistake about language, in which the bad guys agree to follow syntactical and semantical rules known to both parties. Of course, hackerz and others generate the rules embedded in the usage as part of the usage and this means that no automated system can keep up. "Hackerz" is the simplest example because in terms of sound, z is a neighbor of s, due to the topology of our sound production equipment. You can tell the automated system what rules to follow but there is of necessity a boundary which moves but does not disappear.

This presents you with a Hobson's choice. Either you take the time to figure out the rules completely or you use probabilistic models. The first alternative means your results are generally too late for the

SAME reason

large scale projects are so often late. The problem with the second alternative is that the probabilistic model is just as rigid as a deterministic and formal model for the SAME reason that, as von Neumann said, a computer cannot generate a truly random number. It is a form of "night vision" which has the probability that the gear will conceal just what you need to know.

It gets worse, because you've told the bad guy that you are using Enigma or Groove. All he needs to do is buy, steal or reverse engineer your model!

> [...]

Cops keep crime scene details secret. But they do not set up a data system to do so because this presents the possibility that the details can be known. Cops are aware, unlike data systems people, that they are in a "dialogue" with "terrorists" in the sense of a probability that any one of their actions may be known as part of its being recorded.

Ordinary computer users are told on day one that anything they write in e-mail must be treated as if it would appear in the local newspaper. The TIA seems to ignore this simple rule insofar as it encapsulates intelligence procedures in a form that is easy to copy.

Note that its chief Poindexter was unaware in 1987 that his e-mail on the White House PROFS system was not completely erased when he erased his copy, and Congress as a result was able to use his e-mail in their investigation of

his felonious conduct in Irangate.

Poindexter may now realize that there are limits to file deletion, and since 1987 there have been a number of papers on "levels" of file delete.

But more broadly, there is in Poindexter and the Administration a naivete (which is evident in the announcement of the purchase of Groove) about Turing limitations as well as the tendency of large networks to join as the result of one key gateway: a government Internet would become part of the World Wide Web on the day ANY hacker created a simple gateway in a literal sense.

[I generally remove most of the interstitiated lines to which such point-by-point responses allude. If you find this item curious, please refer back to the [earlier message from Jerrold](#). PGN]

TIA: Groove is simply a collaboration tool

Stever Robbins <stever@VentureCoach.com>
Tue, 07 Jan 2003 08:56:21 -0500

I think we're seeing a meta-Risk: the risk of evaluating risks without enough understanding of the tools being discussed. In this case, Groove.

I've been puzzled by the discussion of Groove in TIA. Groove is simply a piece of collaboration software. It lets you create a shared

"workspace" that can contain a threaded discussions, a shared calendar, instant messaging, and shared files. You can also share a plug-in to share other types of documents (for example, I use Groove with the Mindjet "Mind Manager" plug-in, which lets me share mind maps with my colleagues).

It may have been chosen for TIA because Groove is a peer-to-peer collaboration tool, a la the Napsters of the world, rather than hosting a shared space on a central server. So there's no obvious place for terrorists to eavesdrop if they wants to sabotage a Groove workspace; the space is distributed among its members' PCs.

Groove does no detection or analysis of any sort. It's just a framework for sharing information.

Check it out. You can download and use it for free from <http://www.groove.net>. I tried it a few months ago and like it so much I've been using it for a few projects I have going.

One side note: if TIA will depend on Groove, then perhaps those of us in fear for our civil liberties needn't fear. Only about 60% of the people I've had download it seem to be able to install it and get it working. (I think it's written in Java, which apparently isn't as portable as one might wish.)

⚡ Re: TIA, surveillance, and Tolkien

Monty Solomon <monty@roscom.com>

Sat, 4 Jan 2003 13:57:23 -0500

Bush's Year of U.S. Surveillance, Noah Shachtman, wired.com, 2 Jan 2003

It may seem unreasonable, unfair and downright mean-spirited to compare the Bush administration to the minions of Sauron, the granddaddy of evil in The Lord of the Rings trilogy. But here goes.

The executive branch's attempts in 2002 to peer into the lives of Americans were more than a little similar to the exploits of Middle Earth's would-be rulers. Take, for example, the Bush team's most notorious proposal of the year: the Total Information Awareness system. TIA is an "ultra-large, all-source information repository" meant to track citizens' every move, from Web surfing to doctor visits, travel plans to university grades, passport applications to ATM withdrawals.

For J.R.R. Tolkien fans, the scheme sounds eerily familiar. ...

<http://www.wired.com/news/privacy/0,1848,57005,00.html>

⚡ REVIEW: "Building Linux Virtual Private Networks",

Rob Slade <rslade@sprint.ca>

Tue, 7 Jan 2003 08:22:49 -0800

Oleg Kolesnikov/Brian Hatch

BKBLVPNS.RVW 20020916

"Building Linux Virtual Private Networks (VPNs)", Oleg

Kolesnikov/Brian Hatch, 2002, 1-57870-266-6, U\$44.99/C\$69.99/
UK#34.99

%A Oleg Kolesnikov oleg@buildinglinuxvpns.net ok@cc.gatech.edu
%A Brian Hatch bri@buildinglinuxvpns.net brian@onsight.com
%C 201 W. 103rd Street, Indianapolis, IN 46290
%D 2002
%G 1-57870-266-6
%I Macmillan Computer Publishing (MCP)/New Riders
%O U\$44.99/C\$69.99/UK#34.99 800-858-7674 317-581-3743 info@mcp.
com
%O [http://www.amazon.com/exec/obidos/ASIN/1578702666/
robladesinterne](http://www.amazon.com/exec/obidos/ASIN/1578702666/robladesinterne)
%P 385 p.
%T "Building Linux Virtual Private Networks (VPNs)"

Like "Practical UNIX and Internet Security" (cf. BKPRUISC.RVW) this book so thoroughly covers its general field, in this case virtual private networks (VPNs), that it is useful to security people regardless of whether or not they use Linux. There are abundant practical considerations in this work that other volumes ignore.

Part one deals with the basics of VPNs. Chapter one is a good, readable, realistic introduction (and we will accept the mention of 40 bit DES in IPsec as a typo: it is listed as such in the errata at the associated Web site, <http://www.buildinglinuxvpns.net>). The title of chapter two, VPN fundamentals, is oddly both true and not: the items mentioned are not factors of VPNs as such, but aspects and considerations of VPNs that influence network choices, and network configurations that impel VPN architecture.

Part two covers implementing standard VPN protocols. Chapter three provides

a detailed and clear explanation of PPP (Point-to-Point Protocol) over SSH (Secure Shell). PPP over SSL (Secure Sockets Layer)/TLS (Transport Layer Security), in chapter three, outlines the basics, increased security, and scripts for troubleshooting. Excellent coverage of IPsec in general, plus some implementation details in Linux, is in chapter five. Chapter six explains FreeS/WAN from philosophy to source to configuration. There is good analysis of the design and weaknesses of PPTP (Point-to-Point Tunneling Protocol) and how to run it on Linux, in chapter seven.

Part three examines the implementation of nonstandard VPN protocols. Chapter eight looks at the design, options, and setup of VTun. The lightweight cIPE is covered in chapter nine. Designed for user level rather than kernel operation, as well as more modern and robust cryptography, tinc is explained in chapter ten.

I have not found, to date, a book that does a better job of explaining the concepts and operations of virtual private networks. This should become the classic text.

copyright Robert M. Slade, 2002 BKBLVPNS.RVW 20020916
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

<http://victoria.tc.ca/techrev/~rslade> or <http://sun.soci.niu.edu/~rslade>

🔥 REVIEW: "Know Your Enemy", Honeynet Project

Rob Slade <rslade@sprint.ca>

Mon, 30 Dec 2002 08:05:18 -0800

BKKNYREN.RVW 20020916

"Know Your Enemy", Honeynet Project, 2002, 0-201-74613-1,
U\$39.99/C\$59.95

%A Honeynet Project

%C P.O. Box 520, 26 Prince Andrew Place, Don Mills, Ontario
M3C 2T8

%D 2002

%G 0-201-74613-1

%I Addison-Wesley Publishing Co.

%O U\$39.99/C\$59.95 416-447-5101 fax: 416-443-0948

%O [http://www.amazon.com/exec/obidos/ASIN/0201746131/
robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/0201746131/robsladesinterne)

%P 328 p. + CD-ROM

%T "Know Your Enemy: Revealing the Security Tools, Tactics, and
Motives of the Blackhat Community"

I have frequently said that any book with "hack," or any variant thereof, in the title is automatically suspect. This work helps prove my point, first, because the Honeynet Project members have *not* used the term (they refer to attackers as blackhats), and the text also notes the problems with "exploit" type books: they list old and known attacks, most of which are protected against, and say nothing about the attackers and how they work. Chapter one points out the value of "knowing the enemy" and the beginnings of the Honeynet Project.

Part one describes the honeynet. Chapter two explains what a honeynet is, and the difference between one and the traditional honeypots. Details on how a honeynet works, in terms of architecture, policies, and

the risks and responsibilities of operating one, are presented in chapter three. Building a honeynet, in chapter four, presents specific details, although a number have already been given.

Part two concerns the analysis of data collected from the Honeynet. Chapter five, on data analysis, points out the sources of data for logging, much of which has already been discussed. There is some more information on what we can find, but limited explanation of how to interpret it. The discussion of analyzing a compromised system, in chapter six, is more detailed and does a better job of explaining the logs, but relies on a blackhat document, which, while better than most such, still has the holes and gaps that characterize the genre. Additional details are provided in advanced data analysis, plus some material on data that is (and some that is not) useful in packets, plus forensic (data recovery) considerations, in chapter seven. (Interestingly, the Honeynet Project does not seem to be concerned with wiping a drive in order to deny information to blackhats.) Chapter eight examines data recovery tools and some results.

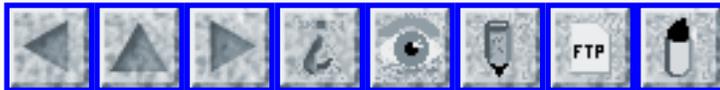
Part three explains what the project has determined about "the enemy" by the types of attacks that have been launched and detected. Chapter nine is a general review of the random nature of attacks, the tools seen, motives theorized, and trends in attacks. The activities and signatures of the Bymer worm are described in chapter ten. An IRC conversation between a

group of blackhats is provided in chapter eleven. While there is some interest in the account, the transcript occupies almost 100 pages (and almost a third of the total length of the book). Chapter twelve suggests the future activities of the Honeynet Project.

Much of the material in the book is repeated, sometimes in a number of places. The text would definitely benefit from a tightening up of the material. In addition, the early examples are not thoroughly explained, making the reader initially feel that only a firewall audit log specialist would be able to understand what is being said. However, most of the book is written clearly and well, and it is definitely worth reading.

copyright Robert M. Slade, 2002 BKKNYREN.RVW 20020916
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

<http://victoria.tc.ca/techrev/~rslade> or <http://sun.soci.niu.edu/~rslade>



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

[ACM](#) Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 49

Weds 15 January 2003

Contents

- [Computer sabotage against Venezuela oil?](#)
[David Wagner](#)
- [Brace for onslaught of new viruses](#)
[NewsScan](#)
- [Y2K+3 bug in Networker](#)
[William D. Colburn](#)
- [Smut hits 'Army Newswatch'](#)
[Monty Solomon](#)
- [How to vote for your favorite California quarter design](#)
[Fred Cohen](#)
- [Hong Kong gym pulls plug on camera cell phones](#)
[Monty Solomon](#)
- [Amazon not checking for sensible values](#)
[Jeremy Epstein](#)
- [Google Search cached a password protected page?](#)
[Colin Sutton](#)
- [Misuse of HTML comments causes missed comments](#)
[Alexander Dupuy](#)
- [Biometric lunch lady](#)
[Richard Akerman](#)

- [Re: PGP.COM cannot handle sales to some US residents](#)
[Stephan Somogyi](#)
 - [REVIEW: "CISSP for Dummies", Lawrence Miller/Peter Gregory](#)
[Rob Slade](#)
 - [REVIEW: "Information Security Policies, Procedures, and Standards", Thomas R. Peltier](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ **Computer sabotage against Venezuela oil?**

David Wagner <daw@cs.berkeley.edu>
Tue, 14 Jan 2003 21:13:37 -0800 (PST)

Oil Daily quoted Ali Rodriguez (head of Venezuela's state oil company):

"[...] we have suffered many acts of sabotage at the terminals, the refiners, and even to some well-heads in Lake Maracaibo. There were even instances of computer hacking which did a lot of damage since much of the operation is centrally controlled by computer."
[Source: *Oil Daily*, vol 53, no 9, 14 Jan 2003]

Does anyone know anything more?

⚡ **Brace for onslaught of new viruses**

"NewsScan" <newsscan@newsscan.com>
Tue, 14 Jan 2003 08:48:22 -0700

Computer users will be plagued with a host of new viruses this year,

particularly worms deployed into instant messaging systems, predicts a senior technology consultant with UK-based Sophos. "Virus writers are most interested in creating the next super Windows worm, spread by e-mail or instant messaging, as these mass-mailing viruses carry the greatest impact," says Graham Cluley. "We expect more executable e-mail-aware worms this year, while more viruses are written which use instant messaging services." Sophos also expects to see an increase in the number of so-called "Backdoor Trojans," which can open up holes in operating systems so that crackers can control them from a remote location. Windows users are particularly at risk, as nine out of 10 of last year's top viruses were spread via e-mail on Windows platforms, with the most prolific being the Klez worm. So far, PDAs and mobile phones have remained largely free of virus problems, says Cluley. "There is no indication yet that we will see an avalanche of new viruses affecting mobile devices -- virus writers are not interested in targeting the mobile phone until it becomes more developed and has a bigger, common platform." [Reuters 14 Jan 2003; NewsScan Daily, 14 Jan 2003]

<http://shorl.com/fikunumubodri>

⚡ Y2K+3 bug in Networker

"William D. Colburn (Schlake)" <wcolburn@nmt.edu>
Fri, 10 Jan 2003 11:19:43 -0700

We currently use NetWorker 6.0.1.Build.174 Turbo/15 as our backup software.

The first Saturday of the new year (4 Jan 2003) it appeared that only one tape was correctly labeled, and that data was appended to previous dumps on some recycled tapes. Now that the second Saturday is upon us, we watched today's tape labelling and saw that NetWorker is labelling the first tape correctly, but then reverting to the label scheme for the backups on 5 Jan 2002.

The risk of this error is almost social engineering. Tomorrow's tapes should be labelled Full.2003.01.11.a, .b, etc. Some tapes labelled as Full.2002.01. will soon be eligible for recycling. We recycle by hand, and if the person doing it didn't know these were mislabeled then we could lose recent backups.

William Colburn, Computer Center, New Mexico Institute of Mining and Technology
wcolburn@nmt.edu <http://www.nmt.edu/tcc/> <http://www.nmt.edu/~wcolburn>

Smut hits 'Army Newswatch'

"monty solomon" <monty@roscom.com>
Thu, 9 Jan 2003 22:34:06 -0500

The town of Webster, NY, is investigating what might have caused a program

about the U.S. Army on its local cable access channel to be interrupted by about 20 minutes of explicit gay porn. [Source: John Kohlstrand, *Rochester Democrat and Chronicle*, 9 Jan 2003; PGN-ed]
http://www.rochesterdandc.com/news/0108story8_news.shtml

⚡ How to vote for your favorite California quarter design

Fred Cohen <fc@all.net>

Tue, 14 Jan 2003 15:55:01 -0800 (PST)

The forms at:

<http://www.caquarter.ca.gov/>

Allow anyone to vote on the appearance of the California quarter. According to my daughter you can vote as many times or as often as you want. The site uses a simple 'FORM NAME="COIN" METHOD="post"' method with parameters like 'NAME="QUARTER" VALUE="16"' (my vote) as parameters.

It is indeed trivial to send in a few hundred votes per second from a modem, thousands from a DSL line or cable modem, and of course if you can afford an OC48, you can probably vote billions of times a day.

I don't think they will use this as their sole decision process, but when it comes to Internet voting, I think this is a shining example of how artistic license can mint a winner.

Fred Cohen <http://all.net/> fc@all.net fc@unhca.com tel/fax:
925-454-0171

Fred Cohen & Associates - University of New Haven - Security

Posture

[However, the new quarters are apparently revitalizing coin collecting, which had grown dormant of late. So, maybe there are also plans to have a similar popularity vote for your favorite state quarter, fully expecting to report votes of 435,829,662,554 for the Rhode Island coin in hopes that it will sell more. PGN]

✶ Hong Kong gym pulls plug on camera cell phones

Monty Solomon <monty@roscom.com>

Wed, 15 Jan 2003 10:58:34 -0500

Warning: use of camera-equipped mobile phones could be hazardous to your health. That's the message going out from at least one chain of health clubs in Hong Kong, where a new generation of cell phones that can take and transmit video and still photos is raising concerns over a new crop of privacy-related issues. Physical, which operates nine gyms in the former British colony, recently posted signs in its Hong Kong facilities forbidding the use of mobile phones in locker rooms. [Source: Reuters item by Doug Young, 14 Jan 2003]

<http://news.lycos.com/news/story.asp?section=OddNews&storyId=623861>

Amazon not checking for sensible values

"Jeremy Epstein" <jepstein@webmethods.com>

Fri, 10 Jan 2003 11:41:29 -0500

There are lots of bugs due to not checking for sensible values, and I found this one amusing. Bret Hartman sent me a copy of his new book "Mastering Web Services Security", and I wanted to recommend it to a friend. So I went to Amazon, which tells me "Availability: This title will be released on December 31, 1969. You may order it now and we will ship it to you when it arrives."

Seems to be missing a sanity check regarding the "to be published date" being in the future.

Google Search cached a password protected page?

"Colin Sutton" <colin@sutton.wow.aust.com>

Sun, 12 Jan 2003 22:30:46 +1100

Searching for SQL help on google

<http://www.google.com.au/search?q=%22ANSI+SQL+CASE%22&hl=en&lr=&ie=UTF-8&oe=UTF-8&start=10&sa=N>

<http://rec.schoolsnet.syd.catholic.edu.au/> I found a link to a password controlled site, but the page and hundreds more on that site are visible in the google cache.

Can a supposedly secure site be cached on google for anyone to see if a person with access permissions uses google to search it?

I don't have access to any such sites, or I'd try it.

Or, perhaps the password protection was added after the site was protected.

Either way, there's a risk.

✶ Misuse of HTML comments causes missed comments

Alexander Dupuy <dupuy@cs.columbia.edu>

Sat, 11 Jan 2003 01:31:08 -0500

My boss sent me (using some version of Outlook) some important mail with comments on several included nested messages, all of which in multipart alternative text and html. Unfortunately, my browser chose the html, which contained lots of microsoft stuff embedded in HTML comments.

Apparently there's a bug in whatever version of Outlook, and the microsoft gunk sometimes omits a closing `<![endif]-->`, which isn't a big deal for the microsoft HTML renderer, but is a big deal for other HTML renderers, since it leaves the HTML comment open, including all of the message text up to the end of the next HTML comment, just before the body text of the first "Original Message".

For microsoft HTML renderers, the missing bit makes no difference, as it is displaying the data even though it is in a comment (I guess it recovers okay from the missing endif), but for people with other HTML

renderers, the
comment is completely invisible. I only saw the included
messages, but none
of my boss's comments (the non-HTML kind).

I only realized that this had happened when one of my co-workers
(who uses
emacs to read his e-mail) replied to the message, and included
some text
that I hadn't seen.

✶ Biometric lunch lady

Richard Akerman <rakerman@bigfoot.com>

Thu, 09 Jan 2003 21:53:02 -0500

In what seems like a remarkably elaborate solution to a simple
problem,

"students will be charged for their lunches with a retina
scanning device"

at a school in England starting in September.

http://www.salon.com/tech/wire/2003/01/09/uk_school/

This brings a whole new meaning to "stealing someone's lunch
money".

✶ Re: PGP.COM cannot handle sales to some US residents (Kabay, [R-22.46](#))

Stephan Somogyi <:ssomogyi@pgp.com>

Sun, 5 Jan 2003 23:04:29 -0800

It distresses me acutely that Dr Kabay did not have the most
friction-free

purchasing experience possible -- my inner Ferengi does so hate it when we hinder a customer from exchanging money for one of our fine products -- and while the above provides all the necessary clues, Dr Kabay unfortunately does not draw the correct conclusions.

As he points out, Dr Kabay is using his StarBand account. This is a satellite-based ISP with a footprint that covers the continental US as well as quite a bit of geography surrounding it. <http://www.starband.com/whatis/> is a helpful source for determining the service's reach.

I am not a professional cartographer, yet it appears to my layman's understanding of geography that one of the above explicitly named seven countries quite likely finds itself within a satellite footprint that extends out to the US Virgin Islands.

Since PGP Corp is located in California, we are subject to US laws. These include the export restrictions overseen by the Department of Commerce in the form of its BIS, the Bureau of Industry and Security, formerly known as the BXA, the Bureau of Export Administration.

If we guess right about a given satellite ISP user, we generate about 40 bucks in revenue. If we guess wrong, we're looking at \$10K+ in fines, and are further subject to administrative actions up to and including "no more export to anywhere for you, ever."

As risk assessment goes, this is not a hand-wringer.

>The customer service agent was very nice and obviously embarrassed
>about this situation and admitted that there are no measures in
>place for dealing with such a technical glitch.

There is no technical glitch. Evidence clearly suggests that our customer service agent may not have had all the facts available to her at the time Dr Kabay called, but the system functioned as designed.

We "fail closed" rather than "fail open" based on having examined the risks inherent in delivering export-controlled software to a world-wide audience. If we cannot ascertain your whereabouts with a reasonable degree of certainty (and StarBand doesn't provide that information as part of the reverse-resolved IP address), we will not deliver software to you and expose ourselves to some rather substantial liability.

>1) Check the IP address BEFORE the user fills out all the forms and
>the credit card gets debited.

I'm delighted that Dr Kabay suggests this course of action, since it provides the opportunity to expose another risk that we've had to take into consideration. It is not feasible to perform such a check before the user fills out the form since it opens us up to a financial denial of service attack.

Performing the necessary checks to determine a buyer's suitability for sale costs PGP Corp money per check. The process involved is not a simple matter of reverse-resolving an IP address. If we were to perform the requisite check prior to accepting the credit card, it would be a trivial

exercise to
launch an attack that's quite expensive to us.

>2) Send the user a CD-ROM to the US address listed in the order.

We are currently investigating this as an alternate delivery method.

>3) Ask the user for strong evidence that they are in fact living in
>the US: e.g., [...]

I cannot imagine that Dr Kabay meant this suggestion seriously. As a non-governmental organization, we have no ability to verify a given driver's license's validity or the whereabouts of its holder, nor are we able to divine what an "appropriate US fax machine" is.

Moreover, it strikes me as ironic to suggest that a company such as PGP Corp, which is committed to security and privacy, put itself in a position where it has to make a determination about what constitutes an authoritative means of location identification, and then verify it.

>b) ask for other corroborating evidence such as a US address
>listing in university or corporate Web sites.

Had Dr Kabay attempted to purchase and download our software from a university or corporation with an unambiguous location, I daresay he would've succeeded.

>RISKS of assuming your automated system is perfect: you lose sales.

We assume no such thing. Our system did, however, operate precisely as it was supposed to in this instance.

RISKS of not erring on the side of caution when it comes to the law: gaining the concerted attentions of the BIS.

Stephan Somogyi, Director of Products, PGP Corporation

★ **REVIEW: "CISSP for Dummies", Lawrence Miller/Peter Gregory**

Rob Slade <rslade@sprint.ca>

Tue, 10 Dec 2002 08:02:38 -0800

BKCISPD.M.RVW 20021029

"CISSP for Dummies", Lawrence Miller/Peter Gregory, 2002,
0-7645-1670-1, U\$39.99/C\$59.99/UK#29.95

%A Lawrence Miller

%A Peter Gregory peter.gregory@hartgregorygroup.com

%C 5353 Dundas Street West, 4th Floor, Etobicoke, ON M9B 6H8

%D 2002

%G 0-7645-1670-1

%I John Wiley & Sons, Inc.

%O U\$39.99/C\$59.99/UK#29.95 416-236-4433 fax: 416-236-4448

%O <http://www.amazon.com/exec/obidos/ASIN/0764516701/>

[robsladesinterne](#)

%P 408 p. + CD-ROM

%T "CISSP for Dummies"

A 'cheat sheet' is bound into the front of the book. It offers some general

advice for taking the CISSP (Certified Information Systems Security

Professional) exam, the most useful aspect of which is to prepare. Most of

the tips are vague, such as the suggestion to budget your time, or review

CISSP resources, without any information about what factors should be

considered in time management or where to find resources. Some tips are overly specific, such as the recommendation that you bring a big bottle of water. (Yes, six hours is a long time for the exam, and, yes, you may need refreshment. The tip does not mention that proctors vary in rigour when applying the exam regulations, and may not allow bottles of water at the test tables. Besides which, only one person may be excused from the room at any one time.)

Part one reviews the CISSP exam itself. At the beginning of chapter one, the authors point out that some CISSP study guides are too hard, and some CISSP study guides are too soft, but this book is just right. Then it moves on to information about (ISC)² (the International Information Systems Security Certification Consortium), arrangements for the exam, and some study tips. The material is more up-to-date than in other CISSP study guides, but the text is badly written, duplicating content and repeating itself, possibly because the structure and organization is weak. The suggestions and information are reasonable, although occasionally questionable: the recommendations for study guides and practice exams are rather weak. Chapter two briefly lists the ten domains of the common body of knowledge (CBK), and is really only an expanded table of contents for the chapters in the next section.

Part two describes the ten domains in detail. Chapter three covers most of access control, but unevenly. Given the constraints that the authors

themselves mention (the CISSP CBK is a mile wide and an inch deep), too much space is devoted to a simplistic set of password choice rules, an excellent (but, in this situation, overlong) review of Kerberos, and a number of jokes which are not going to help candidates remember important points, and may very well confuse the issues. Some material is problematic, such as the discussion of security "domains" that follows the Microsoft networking model rather than the Bell-LaPadula derived structure that the CBK requires, and a baffling non-explanation of the lattice model. (There are also a number of perplexing inclusions, such as a cross-reference to cryptography in the introduction to single sign-on systems.) Telecommunications and network security is presented in chapter four. The authors have used the OSI (Open Systems Interconnection) model to structure the discussion of various technologies: an interesting concept, but one which is flawed by the fact that a number of topics are placed in the wrong level. (Media access and packet switching, for example, are listed in the data link layer, rather than the physical and network layers, respectively.) There are also problematic references to "native" PPP (Point-to-Point Protocol) encryption, and an assertion that ICMP (Internet *Control* Message Protocol) packets are not required for network operations. The basics of security management are covered in chapter five, but very tersely. The major standards are not listed here: the Common Criteria is mentioned briefly in chapter eight (security architecture) but British Standard 7799/ISO

(International Standards Organization) 17799 is not listed at all. The set of roles and responsibilities is short and risk analysis terms are not well defined. This must be considered a serious weakness in the book, since security management is very important in the CISSP exam. Application development is dealt with briefly and poorly: again, this is an area where many CISSP candidates do need extra help, and they won't get it here. System development methods are not discussed at all, and the malware section is full of errors. (Each chapter lists a set of books for extra research: I should note that neither of the virus books listed at the ISC2 site appear on the list for this chapter. In fact, the bibliography is rather short overall: Krutz and Vines "The CISSP Prep Guide" (cf. BKCISSPPG. RVW) which is not much better than the current work, is listed in every set.) There are also odd inclusions from other domains, such as almost a full page devoted to the SYN flood attack, which was adequately explained in a paragraph in chapter four. The material on cryptography, in chapter seven, lists all the terms and technologies, but has poor or non-existent explanations, mathematical errors, and the authors obviously do *not* understand S-boxes. (The process described would not allow for decryption.) There is too much text about CPUs (Central Processing Units), and too little on distributed systems, formal models, and the various evaluation criteria in chapter eight's review of security architecture. Operations security, in chapter

nine, seems to be a collection of random topics, with a fair concentration on audit logs. Chapter ten's overview of Business Continuity Planning (BCP) is not bad, although a bit shy on details. (The vital topic of backups, for example, is mentioned only long enough to say that you should have one, and the various types, with varying strengths and weaknesses, are not discussed at all.) Law, investigation, and ethics is reasonable, although the list of specific privacy laws is probably not too helpful (and I rather suspect that the authors got taken in by the "Desert Storm Virus" myth). Most of the material on physical security, in chapter twelve, appears to have been copied from some other source without much understanding: the sections on visibility, capacitance sensors, and UPSes (Uninterruptible Power Supplies) are among those that contain errors or seem to miss the major points.

Part three is the usual "dummies" "part of tens." Chapter thirteen relists the ten domains. (Didn't we do this already?) Ten other security certifications are recorded in chapter fourteen. Web sites are given in chapter fifteen: three are actually useful. The cheat sheet and chapter one are reprised in sixteen and seventeen. One of the books listed in chapter eighteen ("Security Engineering," by Ross Anderson, cf. BKSECENG. RVW) would be very useful for exam candidates.

Sample test questions are a big part of every CISSP study book (in the case of Peltier and Howard's "The Total CISSP Exam Prep Book," in fact, the

only part). This book has both its own set of questions, and a set from the Boson exams. As I have said elsewhere, the Boson exams are not necessarily wrong, but they are far too simplistic to be considered adequate preparation for the CISSP exam, and the answer guides are completely tied to "Secured Computing" (cf. BKSCDCMP.RVW). If any set of questions are simpler, and therefore less useful, than the Boson set, they are the ones listed in this book. And, like the Boson collection, the answers are completely self-referential.

Like Andress' "CISSP Exam Cram" (cf. BKCISPEC.RVW), this text does sometimes simply list the terminology, although Miller and Gregory are somewhat more complete and do provide greater explanations of the domains themselves. It would be hard to make a distinction between this volume and "Secured Computing": Miller and Gregory provide *some* outside references but Endorf makes fewer errors. As previously noted, Krutz and Vines do not give the reader much in the way of explanatory material, but they do cover the domains more comprehensively than the current work. Harris' "CISSP All-in-One Certification Exam Guide" is, as noted (cf. BKCISPA1.RVW), the one guide that might get you through the CISSP exam, albeit not necessarily with high marks: Miller and Gregory might get you through, but only if you stood a pretty good chance without the volume.

copyright Robert M. Slade, 2002 BKCISPDM.RVW 20021029
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

<http://victoria.tc.ca/techrev/~rslade>

or

<http://sun.soci.niu.edu/>

REVIEW: "Information Security Policies, Procedures, and Standards",

Rob Slade <rslade@sprint.ca>

Wed, 4 Dec 2002 08:43:30 -0800

Thomas R. Peltier

BKISPPAS.RVW 20020923

"Information Security Policies, Procedures, and Standards",
Thomas R.

Peltier, 2002, 0-8493-1137-3

%A Thomas R. Peltier

%C 920 Mercer Street, Windsor, ON N9A 7C2

%D 2002

%G 0-8493-1137-3

%I Auerbach Publications

%O U\$69.95 +1-800-950-1216 auerbach@wgl.com orders@crcpress.com

%O <http://www.amazon.com/exec/obidos/ASIN/0849311373/>

[robsladesinterne](#)

%P 297 p.

%T "Information Security Policies, Procedures, and Standards"

Chapter one provides vague meanderings about information protection fundamentals. The author's opinion about how to write is given in chapter two. In the ultimate triumph of style over substance, this drafting advice is given before any examination of actual policy development. Chapter three defines policy and some related topics with lots of verbiage and overly lengthy examples. There are lots of sample mission statements in chapter four, although it is not

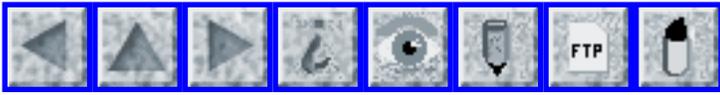
really
apparent why we are talking about this particular topic. The
structure of chapter five, dealing with standards, is very
confused,
and the purpose of the examples given is unclear. (There is
also an
extremely odd assertion that standards, which are by definition
rigid,
must be "flexible.") We are given more writing advice,
supposedly in
aid of procedures, in chapter six. Chapter seven talks about
information classification for a few paragraphs and then lays
out a
thirty page example. Random security thoughts and banal training
ideas make up the security awareness program in chapter eight.
Generic project management advice is in chapter nine. Chapter
ten
contains suggested topics for a security policy. What the book
said
is repeated in chapter eleven.

The appendices include a very short sample policy, and a policy
development checklist.

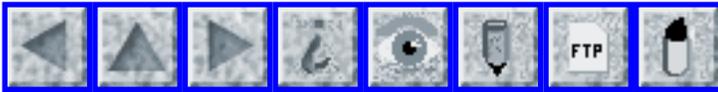
Barman's "Writing Information Security Policies" (cf. BKWRINSP.
RVW)
provides far better advice on both the process and the topics to
be
covered in creating a security policy. Even "Information
Security
Policies Made Easy" (cf. BKISPME.RVW) is better, for all that
people
tend to misuse it. Peltier's book provides little of use to the
harried security manager.

copyright Robert M. Slade, 2002 BKISPPAS.RVW 20020923
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

<http://victoria.tc.ca/techrev> or <http://sun.soci.niu.edu/~rslade>



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

[ACM](#) Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 50

Saturday 18 January 2003

Contents

- [CLU sees a growing 'surveillance monster'](#)
[NewsScan](#)
- [Michelin to embed electronic ID tags in tires](#)
[Monty Solomon](#)
- [Junked hard drives yield lots of personal data](#)
[NewsScan](#)
- [Girl suffers burns after laptop explodes](#)
[Monty Solomon](#)
- [Cash machine error goes unchecked](#)
[Tim Storer](#)
- [Exchange/Outlook being "helpful"](#)
[Pete Carah](#)
- [Equifax "security"](#)
[Yakov Shkolnikov](#)
- [Lexmark DMCA lawsuit temporary restraining order](#)
[Monty Solomon](#)
- [DMCA vs. The Garage Door Opener](#)
[Fred von Lohmann via Declan McCullagh](#)
- [Re: Sophos "more viruses" warning: grain of saakolt?](#)
[Denis Haskin](#)

- [REVIEW: "Building Secure Software", John Viega/Gary McGraw](#)
[Rob Slade](#)
 - [REVIEW: "Network Security", Charlie Kaufman/Radia Perlman/Mike Speciner](#)
[Rob Slade](#)
 - [REVIEW: "Web Security, Privacy and Commerce", Garfinkel/Spafford](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ **ACLU sees a growing 'surveillance monster'**

"NewsScan" <newsscan@newsscan.com>

Thu, 16 Jan 2003 09:23:09 -0700

In a new report called "Bigger Monster, Weaker Chains," the American Civil Liberties Union says that there is a rapidly growing "American Surveillance Society" brought about by "a combination of lightning-fast technological innovations and the erosion of privacy protections" threatening "to transform Big Brother from an oft-cited but remote threat into a very real part of American life." This "surveillance monster" includes, among other things, cameras monitoring public spaces, proposals for databases filled with personal information on U.S. citizens, and anti-terrorist legislation allowing the government to demand that libraries turn over reading histories of their patrons. Yet the report asserts that these monsters don't even have to be real for them to be terrifying: "It is not just the reality of government surveillance that chills free expression and the freedom that Americans enjoy. The same negative effects come

when we are
constantly forced to wonder whether we might be under
observation." [AP/*USA

Today 16 Jan 2003; NewsScan Daily, 16 Jan 2003]

[http://www.usatoday.com/tech/news/2003-01-16-privacy-threats_x.
htm](http://www.usatoday.com/tech/news/2003-01-16-privacy-threats_x.htm)

⚡ Michelin to embed electronic ID tags in tires

Monty Solomon <monty@roscom.com>

Fri, 17 Jan 2003 03:09:56 -0500

Michelin plans to embed technology in its tires that would allow
the tires
to communicate wirelessly to the car, sending pressure readings,
etc., to
the dashboard computer, using an antenna and an integrated
circuit the size
of a match head. Proponents of such RFID tags, which store,
send and
receive data through weak radio signals, believe they will one
day replace
bar codes and revolutionize the way that inventories are tracked
and
consumer products are designed once their price falls far enough.
[Source: Reuters item 14 Jan 2003; PGN-ed]

[http://www.reuters.com/newsArticle.jhtml?
type=technologyNews&storyID=2045403](http://www.reuters.com/newsArticle.jhtml?type=technologyNews&storyID=2045403)

[Also noted by Richard M. Smith]

⚡ Junked hard drives yield lots of personal data

"NewsScan" <newsscan@newsscan.com>

Thu, 16 Jan 2003 09:23:09 -0700

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; Newsscan Daily, 16 Jan 2003
<http://apnews.excite.com/article/20030116/D70JBBBG0.html>

★ Girl suffers burns after laptop explodes

Monty Solomon <monty@roscom.com>
Fri, 17 Jan 2003 01:14:33 -0500

A 15-year-old girl suffered second-degree burns to her hands and thighs after the laptop she was using exploded. [Source: Tim Richardson, *The Register*, 16 Jan 2003]
<http://www.theregister.co.uk/content/54/28899.html>

✂ Cash machine error goes unchecked

Tim Storer <tws@dcs.st-and.ac.uk>

Thu, 16 Jan 2003 13:19:30 +0000

A story widely reported in the UK news today (Thursday 16/1/2003) e.g.

http://www.guardian.co.uk/uk_news/story/0,3604,875749,00.html

and also

<http://www.telegraph.co.uk/news/main.jhtml?xml=/opinion/news/2003/01/16/ncash16>

regarding a family who discovered errors in a cash machine whose software had recently been upgraded. They were able to obtain unlimited cash from the machine (some 135,000 pounds) by typing in random PIN numbers.

An issue not included in all the reports was that the family allegedly contacted the building society to report the error (this was reported in the print edition of the Metro, a free newspaper supplied on the UK's public transport infrastructure). Only when the society failed to take action did the family begin exploiting the error.

The risk here (assuming the family did indeed report the fault) would be the failure of the society to implement remedial action when notified of a problem, perhaps due to a lack of procedure for handling such information.

This is quite apart from the clearly inadequate testing of the software added

to the cash machine in the first place.

✶ Exchange/Outlook being "helpful"

Pete Carah <pete@ns.altadena.net>

Sat, 18 Jan 2003 11:40:15 -0800 (PST)

I don't know if this has been covered before, but I have a correspondence going with someone who uses Exchange for his mail.

I have a procmail filter that files mail containing an html tag (the opening html identifier, not just any html tag) in a box labelled spam, which I then peruse about weekly. (and just discards any containing both an html and script tag...)

He complains that I don't answer him timely, and that he has configured his mailer to not send html. This appears to be the case; his messages to me are not put in html form.

The zinger here, is that my quoted message in his reply is in html form, identified as "converted from text/plain", (in the DTD line, I found the conversion having been done by the exchange server) "We're Microsoft, and we're here to help you"...

I don't know if he can suppress that one, either; perhaps by not quoting my incoming message (which should be edited anyhow; I don't like postquotes since they tend to grow uncontrollably).

✶ Equifax "security"

Yakov Shkolnikov <yshkolni@EE.Princeton.EDU>

Sat, 18 Jan 2003 10:50:47 -0500 (EST)

I sometimes wonder why some sites use 128 bit encryption. For example: I just ordered my credit report from Equifax (www.equifax.com). When I completed the order, it sent me to the order confirmation page with my username and password as clear text in the URL. The next day I get a e-mail confirming my order with my password in plain text. RISKS are obvious.

✶ Lexmark DMCA lawsuit temporary restraining order

"monty solomon" <monty@roscom.com>

Thu, 9 Jan 2003 22:47:12 -0500

Lexmark lawsuit seeks to defend intellectual property rights while preserving customers' rights to choose

As a result of a Lexmark International, Inc. lawsuit against Static Control Components, Inc., for violation of the Copyright Act and the Digital Millennium Copyright Act, the federal district court in Lexington, Ky., issued a temporary order - agreed to by Static Control - requiring Static Control to immediately cease making, selling, or otherwise trafficking in

the "Smartek(TM)" microchip for the toner cartridges developed for the Lexmark T520/522 and T620/622 laser printers. The order is in effect until Lexmark's motion for a preliminary injunction is heard by the Court. Lexmark's complaint alleges that the Smartek(TM) microchips incorporate infringing copies of Lexmark's copyrighted software and are being sold by Static Control to defeat Lexmark's technological controls, thereby allowing the unauthorized access to Lexmark's protected software programs and the unauthorized remanufacturing of Lexmark "Prebate(TM)" toner cartridges.

[Source: PRNewswire-FirstCall, 9 Jan 2003; PGN-ed]

<http://www.prnewswire.com/cgi-bin/stories.pl?ACCT=104&STORY=/www/story/01-09-2003/0001869517>

DMCA vs. The Garage Door Opener

Declan McCullagh <declan@well.com>

Wed, 15 Jan 2003 22:05:04 -0500

[I've copied the attorneys for the plaintiffs in case they wish to reply to Fred. For their reference: Politech is a moderated discussion forum populated by many members of the legal community, and I attempt to include all reasonable, well-stated views. --Declan]

Date: Wed, 15 Jan 2003 18:48:21 -0800

Subject: DMCA v garage door openers

>From: Fred von Lohmann EFF <fred@eff.org>

To: Declan McCullagh <declan@well.com>

In the latest bit of DMCA lunacy, copyright guru David Nimmer turned me onto a case that his firm is defending, where a garage door opener company (The Chamberlain Group) has leveled a DMCA claim (among other claims) against the maker of universal garage door remotes (Skylink). Yet another case where the anti-circumvention provisions of the DMCA are being used to impede legitimate competition, similar to the Lexmark case. Not, I think, what Congress had in mind when enacting the DMCA.

The Complaint:

http://www.eff.org/IP/DMCA/20030113_chamberlain_v_skylink_complaint.pdf

The Amended Complaint:

http://www.eff.org/IP/DMCA/20030114_chamberlain_v_skylink_amd_complaint.pdf

The Summary Judgment Motion:

http://www.eff.org/IP/DMCA/20030113_chamerlain_v_skylink_motion.pdf

Attorneys for Skylink are (both at the Orange County offices of Irell

& Manella, a large law firm):

"Nobles, Kimberley" <KNobles@irell.com>

"Greene, Andra" <AGreene@irell.com>

Fred von Lohmann, Senior Intellectual Property Attorney,
Electronic Frontier Foundation fred@eff.org +1 (415) 436-9333
x123

⚡ Re: Sophos "more viruses" warning: grain of salt? ([RISKS-22.49](#))

Denis Haskin <denis@haskinferguson.net>

Wed, 15 Jan 2003 21:16:29 -0500

Shouldn't a warning that "Computer users will be plagued with a host of new viruses this year" be taken with a grain of salt when it comes from a company whose business is selling anti-virus software?

REVIEW: "Building Secure Software", John Viega/Gary McGraw

Rob Slade <rslade@sprint.ca>

Thu, 16 Jan 2003 08:01:41 -0800

BKBUSCSW.RVW 20021124

"Building Secure Software", John Viega/Gary McGraw, 2002,
0-201-72152-X, U\$54.99/C\$82.50

%A John Viega www.buildingsecuresoftware.com

%A Gary McGraw www.buildingsecuresoftware.com

%C P.O. Box 520, 26 Prince Andrew Place, Don Mills, Ontario
M3C 2T8

%D 2002

%G 0-201-72152-X

%I Addison-Wesley Publishing Co.

%O U\$54.99/C\$82.50 416-447-5101 fax: 416-443-0948

%O <http://www.amazon.com/exec/obidos/ASIN/020172152X/>

robsladesinterne

%P 493 p.

%T "Building Secure Software: How to Avoid Security Problems
the
Right Way"

The "right way" of the subtitle is, of course, designing and building a product correctly the first time. The preface states that the book

is concerned with broad principles of systems development, and so does not cover specialized topics such as code authentication and sandboxing. It also points out that software vendors are effectively exempt from liability, and so have no reason to produce secure or reliable software.

Chapter one is an introduction to software security, with an overview of related topics and considerations. Managing software security risks, in chapter two, looks at good practices in the system development life cycle, the position of the security engineer in development, and standards. The authors point out problems in common security "solutions," mostly dealing with authentication, in chapter three. The common myths about the security of open and closed source systems are examined in chapter four. Instead of a checklist of thousands of security items (that likely won't be of much use anyway), chapter five presents ten guiding principles which will probably catch most problems. The list is not a panacea: the first principle is to secure the weakest link, and it takes lots of forethought to design this for type of factor in advance. Auditing software, in chapter six, is more about security assessments being conducted at various stages in the process, for example, using attack trees at the design stage.

The preface states that the book is divided into two parts, conceptual and implementation, and, although there is no formal division, this is probably the beginning of part two. Chapter seven looks at buffers overflows, always and still the most common software security

problem.

This book, it must be assumed, is written primarily for a programming audience, and yet the first part has presented concepts very clearly without necessarily getting into code examples. At this point, however, the material is definitely written for advanced C (and specifically UNIX) programmers, and the basic concepts are sometimes hidden in the details. Access control, primarily in UNIX systems, although with some mention of special capabilities in Windows NT, is the topic of chapter eight. Chapter nine deals with race conditions, including the familiar "time of check versus time of use" problem, although most of the material is limited to file access concerns. There is an excellent and thorough discussion of pseudo random number generation in chapter ten. Applying cryptography, in chapter eleven, stresses the fact that you shouldn't "roll your own," helps out by reviewing publicly available cryptographic code libraries, and even examines the drawbacks of one-time pads. Managing trust and input validation, in chapter twelve, emphasizes input concerns to the point that an important element is possibly buried: in the modern environment, you not only have to trust the goodwill of an entity, but also its ability to defend itself, so as not to become part of an attack against you. Password authentication, in chapter thirteen, promotes randomly chosen passwords. Given a work directed at programming I suppose this is understandable, but recent research has shown that "well chosen" passwords are as easy to remember as naive, and as secure as random. Chapter fourteen is an overview of the basic

aspects of database security, although it only touches on the more advanced topics of this specialized field. Client-side security concentrates on copy protection and other anti-piracy measures in chapter fifteen. Some means of establishing a connection through a firewall are examined in chapter sixteen.

While I can understand and sympathize with the desire to give examples of specific code in dealing with implementation details, there are a number of major concepts covered in the latter part of the book which would have been more accessible to non-programmers had they been dealt with as tutorially as in the first part. Still, the book has a great deal to teach programmers about security and reliability, and security professionals about the requirements of the development process.

copyright Robert M. Slade, 2002 BKBUSCSW.RVW 20021124
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

<http://victoria.tc.ca/techrev/~rslade> or <http://sun.soci.niu.edu/~rslade>

⚡REVIEW: "Network Security", Charlie Kaufman/Radia Perlman/ Mike Speciner

Rob Slade <rslade@sprint.ca>
18 Jan 2003

BKNTWSEC.RVW 20021106

"Network Security", Charlie Kaufman/Radia Perlman/Mike Speciner,
2002,
0-13-046019-2, U\$54.99/C\$85.99

%A Charlie Kaufman ckaufman@usibm.com
%A Radia Perlman radia@alum.mit.edu
%A Mike Speciner ms@alum.mit.edu
%C One Lake St., Upper Saddle River, NJ 07458
%D 2002
%G 0-13-046019-2
%I Prentice Hall
%O U\$54.99/C\$85.99 201-236-7139 fax 201-236-7131
mfranz@prenhall.com
%O [http://www.amazon.com/exec/obidos/ASIN/0130460192/
robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/0130460192/robsladesinterne)
%P 713 p.
%T "Network Security: Private Communication in a Public World,
2e"

For communications security, this is the text. As well as solid conceptual background of cryptography and authentication, there is overview coverage of specific security implementations, including Kerberos, PEM (Privacy Enhanced Mail), PGP (Pretty Good Privacy), IPsec, SSL (Secure Sockets Layer), AES (Advanced Encryption Standard), and a variety of proprietary systems. Where many security texts use only UNIX examples, this one gives tips on Lotus Notes, NetWare, and Windows NT.

Chapter one is an introduction, with a brief primer on networking, some reasonable content on malware, and basic security models and concepts.

Part one deals with cryptography. The foundational concepts are covered in chapter one. Symmetric encryption, in chapter three, is presented in terms of the operations of DES (Data Encryption Standard), IDEA (International Data Encryption Algorithm), and AES.

Chapter four details the major modes of DES. The algorithms for a number of hash functions and message digests are described in chapter

five. Asymmetric algorithms, such as RSA (Rivest-Shamir-Adleman) and Diffie-Hellman, are explained in chapter six, although one could wish for just slightly more material, such as actual numeric computations, that might reach a wider audience. The number theory basis of much of modern encryption is provided as well, in chapter seven. More, including a tiny bit on elliptic curves, is given in chapter eight.

Part two covers authentication. The general problems are outlined in chapter nine. Chapter ten looks at the traditional means of authenticating people: something you know, have, or are. Various problems in handshaking are reviewed in chapter eleven. Chapter twelve describes some strong protocols for passwords.

Part three examines a number of security standards. Kerberos gets two whole chapters, since we are provided with not only concepts but actual packets: version 4 in thirteen and 5 in fourteen. PKI (Public Key Infrastructure) terms, components, and mechanisms are outlined in chapter fifteen. The basic problems in real-time communications security are delineated in chapter sixteen. Chapter seventeen examines the authentication and encryption aspects of IPsec, while chapter eighteen deals with key exchange packets. SSL and TLS (Transport Layer Security) are described in chapter nineteen.

Part four concentrates on electronic mail. Chapter twenty lays out the major concerns and problems. Chapter twenty one discusses PEM and S/MIME (Secure Multipurpose Internet Mail Extensions). PGP is covered in chapter twenty two.

Part five contains miscellaneous topics. Chapter twenty three looks

at firewalls, twenty four at a variety of specific security systems, and twenty five at Web issues. Folklore, in chapter twenty six, briefly lists a number of simple "best practices" that aren't generally part of formal security literature.

The explanations are thorough and well written, with a humour that illuminates the material rather than obscuring it. The organization of the book may be a bit odd at times (the explanation of number theory comes only after the discussion of encryption that it supports), but generally makes sense. (It is, sometimes, evident that later text has created chapters that are slightly out of place.) The end of chapter "homework" problems are well thought out, and much better than the usual reading completion test. If there is a major weakness in the book, it is that the level of detail seems to vary arbitrarily, and readers may find this frustrating. Overall, though, this work provides a solid introduction and reference for network security related topics and technologies.

copyright Robert M. Slade, 1996, 2002 BKNTWSEC.RVW 20021106
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com
<http://victoria.tc.ca/techrev/~rslade> or <http://sun.soci.niu.edu/~rslade>

⚡ REVIEW: "Web Security, Privacy and Commerce", Garfinkel/Spafford

Rob Slade <rslade@sprint.ca>
Wed, 15 Jan 2003 08:03:00 -0800

BKWBSPCM.RVW 20021106

"Web Security, Privacy and Commerce", Simson Garfinkel/Gene Spafford,

2002, 0-596-00045-6, U\$44.95/C\$67.95

%A Simson Garfinkel simsong@aol.com

%A Gene Spafford spaf@cs.purdue.edu

%C 103 Morris Street, Suite A, Sebastopol, CA 95472

%D 2002

%G 0-596-00045-6

%I O'Reilly & Associates, Inc.

%O U\$44.95/C\$67.95 800-998-9938 707-829-0515 nuts@ora.com

%O <http://www.amazon.com/exec/obidos/ASIN/0596000456/>

[robsladesinterne](#)

%P 756 p.

%T "Web Security, Privacy and Commerce"

Anyone who does not know the names Spafford and Garfinkel simply does

not know the field of data security. The authors, therefore, are well

aware that data security becomes more complex with each passing week.

This is, after all, the second edition of what was originally published under the title "Web Security and Commerce," and, while it

is still recognizable as such, the work is essentially completely re-

written. The authors note, in the Preface, that the book cannot hope

to cover all aspects of Web security, and therefore they concentrate

on those topics that are absolutely central to the concept, and/or not

widely available elsewhere. Works on related issues are suggested

both at the beginning and end of the book.

A greatly expanded part one introduces the topic, and the various factors involved in Web security. Chapter one is a very brief overview of Web security considerations and requirements, with some

material on general security concepts and risk analysis. The

underlying architecture of the Web is examined in chapter two, although this is basically limited to Internet structures. (While the material is quite informative, perhaps some examples of HTTP [HyperText Transfer Protocol] would add value.) Cryptography is explained reasonably well in chapter three: there is no in-depth discussion of cryptographic algorithms, but these details can be readily found in other works. Chapter four deals with cryptographic uses, and also with legal restrictions. The concepts and limitations of SSL (Secure Sockets Layer) and TLS (Transport Layer Security) are given in chapter five, although the operational details are not covered. Chapter six starts out with a general discussion of identification and authentication, but then gets bogged down in the details of using PGP (Pretty Good Privacy). The coverage of digital certificates, in chapter seven, is likewise constricted by a dependence upon system technicalities.

Part two concerns the user.

Chapter two looks at the various possible problems with browsers, not all of which are related to Web page programming. Chapter eight looks analytically at the possible invasions of privacy that can occur on the Web. Some non-technical techniques of protecting your privacy, such as good password choice, are described in chapter nine, with various technical means listed in chapter ten. Chapter eleven reviews backups and some physical protection systems. ActiveX and the limitations of authentication certificates, as well as plugins and Visual Basic, are thoroughly explored in chapter twelve. Java security is only marginally understood by many "experts," and not at all by users, so the coverage in chapter thirteen is careful to point

out the difference between safety, security, and the kind of security risks that can occur even if the sandbox *is* secure.

Part three details technical aspects of securing Web servers. Chapter

fourteen looks at physical security and disaster recovery measures.

Traditional host security weaknesses are reviewed in chapter fifteen.

Rules for secure CGI (Common Gateway Interface) and API (Application

Programmer Interface) programming are promulgated in chapter sixteen,

along with tips for various languages. More details on the server-

side use of SSL is given in chapter seventeen. Chapter eighteen looks

at specific strengthening measures for Web servers. You legal options

for prosecuting a computer crime is reviewed in chapter nineteen.

Commercial and societal concerns in regard to content are major areas

in Web security, so part six reviews a number of topics related to

commerce, as well as other social factors. Chapter twenty discusses a

number of technical access control technologies, by system. Obtaining

a client-side certificate is described in chapter twenty one.

Microsoft's Authenticode system is reviewed yet again in chapter twenty two. Censorship and site blocking are carefully examined in

chapter twenty three. Privacy policies, systems, and legislation are

reviewed in chapter twenty four. Chapter twenty five looks at current

non-cash payment systems, and the various existing, and proposed, digital payment systems for online commerce. Having already studied

criminal problems earlier, the book now turns to civil and intellectual property issues, such as copyright, in chapter

twenty
six.

Although it has almost nothing to do with Web security as such, I very much enjoyed Appendix A, Garfinkel's recounting of the lessons learned in setting up a small ISP (Internet Service Provider). (I suppose that this could be considered valid coverage of Web commerce.) The other appendices are more directly related to the topic, including the SSL protocol, the PICS (Platform for Internet Content Selection) specification, and references.

Although the material has been valuably expanded and updated, some of the new content is less worthwhile. The extensive space given to specific products will probably date quickly, although the surrounding conceptual text will continue to provide helpful guidance. Certainly for anyone dealing with Web servers or running ISPs, this is a reference to consider seriously.

copyright Robert M. Slade, 1998, 2002 BKWBSPCM.RVW 20021106
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com
<http://victoria.tc.ca/techrev> or <http://sun.soci.niu.edu/~rslade>



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

[ACM](#) Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 51

Sunday 26 January 2003

Contents

- [Keep it secret, stupid!](#)
[Matt Blaze](#)
- [DoD offering admin privileges on .mil Web sites](#)
[Thomas C Greene via Fuzzy Gorilla](#)
- [A. Guadamuz: Trouble with Prime Numbers: DeCSS, DVD, ...](#)
[Monty Solomon](#)
- [Drunk driver hack](#)
[David Wj Stringer-Calvert](#)
- [TurboTax 'activation' annoys users](#)
[Monty Solomon](#)
- [Spam continues to increase](#)
[Monty Solomon](#)
- [Canadian Centre for Identity Theft?](#)
[Richard Akerman](#)
- [NASTAR web site provides personal skier information to anyone](#)
[Robert H'obbes' Zakon](#)
- [Re: Hard-coded calendar dates](#)
[John Sullivan](#)
- [REVIEW: "Internet Cryptography", Richard E. Smith](#)
[Rob Slade](#)

● [REVIEW: "Cryptography Decrypted", H. X. Mel/Doris Baker](#)

[Rob Slade](#)

● [Info on RISKS \(comp.risks\)](#)

⚡ **Keep it secret, stupid!**

Matt Blaze <mab@research.att.com>

Sun, 26 Jan 2003 17:46:49 -0500

Last year, I started wondering whether cryptologic approaches might be useful for the analysis of things that don't use computers. Mechanical locks seemed like a natural place to start, since they provided many of the metaphors we used to think about computer security in the first place.

So I read everything I could get my hands on about locks, which included most of the available open literature and at least some of the "closed" literature of that field. Once I understood the basics, I quickly discovered, or more accurately re-discovered, a simple and practical rights amplification (or privilege escalation) attack to which most master-keyed locks are vulnerable. The attack uses access to a single lock and key to get the master key to the entire system, and is very easy to perform. For details, see

<http://www.crypto.com/masterkey.html>

I wrote up the attack, in a paper aimed more at convincing computer scientists that locks are worth our attention than anything else (I called

it "Rights amplification in master-keyed mechanical locks"). As I pointed out in the paper, surely I could not have been the first to discover this -- locksmiths, criminals, and college students must have figured this out long ago. Indeed, several colleagues mentioned that my paper reminded them of their college days. There is considerable evidence that similar methods for master key decoding have been discovered and rediscovered over the years, used illicitly and passed along as folklore (several people have unearthed Internet postings dating back as much as 15 years describing how to make master keys). Curious college students -- and professional burglars -- have long been able to get their hands on master keys to the places that interest them.

But the method does not seem to appear in the literature of locks and security, and certainly users of master keyed locks did not seem to know about this risk. I submitted the paper to a journal and circulated it to colleagues in the security community. Eventually, the paper reached the attention of a reporter at the New York Times, who wrote it up in a story on the front page of the business section last week.

The response surprised me. For a few days, my e-mail inbox was full of angry letters from locksmiths, the majority of which made both the point that I'm a moron, because everyone knew about this already, as well as the point that I'm irresponsible, because this method is much too dangerous to publish. A few managed to also work in a third point, which is

that the method couldn't possibly work because obviously I'm just some egghead who doesn't know anything about locks.

Those letters, with their self-canceling inconsistency, are easy enough to brush aside, but there seems to be a more serious problem here, one that has led to a significant real-world vulnerability for lock users but that is sadly all too familiar to contemporary observers of computer security.

The existence of this method, and the reaction of the locksmithing profession to it, strikes me as a classic instance of the complete failure of the "keep vulnerabilities secret" security model. I'm told that the industry has known about this vulnerability and chosen to do nothing -- not even warn their customers -- for over a century. Instead it was kept secret and passed along as folklore, sometimes used as a shortcut for recovering lost master keys for paying customers. If at some point in the last hundred years this method had been documented properly, surely the threat could have been addressed and lock customers allowed to make informed decisions about their own security.

The tragic part is that there are alternatives. There are several lock designs that turn out to resist this threat, including master rings and bicentric locks. While these designs aren't perfect, they resist completely the adaptive oracle attack described in my paper. It's a pity that stronger alternative designs have been allowed to die a quiet death in the

marketplace while customers, ignorant of the risks, have spent over a hundred years investing in inferior systems.

Although a few people have confused my reporting of the vulnerability with causing the vulnerability itself, I can take comfort in a story that Richard Feynman famously told about his days on the Manhattan project. Some simple vulnerabilities (and user interface problems) made it easy to open most of the safes in use at Los Alamos. He eventually demonstrated the problem to the Army officials in charge. Horrified, they promised to do something about it. The response? A memo ordering the staff to keep Feynman away from their safes.

🔥 DoD offering admin privileges on .mil Web sites

"Fuzzy Gorilla" <fuzzygorilla@euroseek.com>
Sun, 26 Jan 2003 14:29:34 -0500

DoD offering admin privileges on .mil Web sites
**The Register*, Thomas C Greene, 24 Jan 2003*

Care to register a .mil Web site of your own for free? The DoD has gone out of its way to make it a snap. An unbelievably badly-protected admin interface welcomes you to register whatever domain you please (<http://Rotten.mil> anyone?), or edit anything they've already got. The interface is so ludicrously unprotected that it's been cached by Google and fails to mention that you must be authorized to muck about with

it.
Incredibly, default passwords are cheerfully provided on the page.

Following an anonymous tip from an observant Reg reader, we've encountered the page in question in the Google cache, and after a bit of our own poking about have also discovered an equally unprotected (and Google-cached) admin interface encouraging us to add a new user, like ourselves, say, which requires no authentication.

All you have to do is find that page and you can set yourself up with a user account, manage your new .mil Web site, fiddle about with other people's .mil Web sites, and generally make an incredible nuisance of yourself. We are, of course, straining against every natural, journalistic impulse in our beings by neglecting to mention any useful search strings with which to find it.

Another unprotected and cached page, this one discovered by our tipster, lists traffic to a major DoD Web site by URL/IP address. This worries us because it may list .mil sites and networked DoD machines that are not public, not hotlinked anywhere, and which might contain (or be networked with other machines that contain) sensitive data. Merely knowing that all those URLs and IP addys are valid and owned by DoD would give a significant advantage to attackers by narrowing their target area dramatically.

We have e-mailed the person who manages these sites - twice in fact - but so

far have not been graced with a reply. We were hoping that they might be inclined to fix this mess quickly so that we could safely include the details in our report. Unfortunately we have to withhold them until we're confident that these security snafus are under control.

Ironically, US Defense Secretary Donald Rumsfeld recently ordered DoD to purge military Web sites of information that might benefit evildoers. That's all well and good, but it might behoove the DoD to stop offering them admin privileges first.

<http://212.100.234.54/content/55/29026.html>

✶ A. Guadamuz: Trouble with Prime Numbers: DeCSS, DVD, ...

Monty Solomon <monty@roscom.com>

Fri, 24 Jan 2003 13:39:23 -0500

A. Guadamuz

Trouble with Prime Numbers: DeCSS, DVD and the Protection of Proprietary Encryption Tools

**The Journal of Information, Law and Technology* (JILT), 2002 (3)*

Andrés Guadamuz González

Law Lecturer

University of Edinburgh

a.guadamuz@ed.ac.uk

Abstract

The DVD video format has become one of the most important developments in the home entertainment market since the popularisation of the

magnetic video recording. The film industry delivered this format with a built in security system which was supposed to avoid illegal copying of the discs, much as what is taking place with the music CD and the almost indiscriminate copying of music into MP3 format over the Internet. This was achieved by means of encryption technology.

This essay deals with the cracking of DVD encryption and its further diffusion as a computer programme named DeCSS, which has been made available over the Internet in various formats, including t-shirts and a numerical representation of the code. There are three court cases based on the online posting of this programme, two in the United States and one in Norway. The article starts by describing the technology involved, as it is felt by the author that some of these technical issues are of importance to the legal implications of the case and should be understood properly. The article then deals with the developments in all of the three cases up to this date. The essay then finishes with a look at the legal issues involved, including hyper-linking, trade secrets, freedom of speech and the translation of DeCSS into numerical format.

This is a Refereed article published on 6 December 2002.

<http://elj.warwick.ac.uk/jilt/02-3/guadamuz.html>

Drunk driver hack

"David Wj Stringer-Calvert" <david.stringer-calvert@sri.com>

Wed, 22 Jan 2003 22:22:35 -0800

A 19-year-old in Besancon, France, was arrested for drunk driving. Arriving for his court hearing, he discovered an unattended computer, and proceeded to erase his record -- replacing it with a winking smiley face. The judge was not amused, and gave him a three-month suspended prison sentence, a \$425 fine, and a three-month suspension of his driving license. [Source: Reuters item, From CNN.com, 21 Jan 2003; PGN-ed]

⚡ TurboTax 'activation' annoys users

Monty Solomon <monty@roscom.com>

Sun, 26 Jan 2003 00:25:26 -0500

A new "product activation" system in many 2003 editions of Intuit Inc.'s TurboTax software prevents people from letting anyone else use the CD-ROM on another computer in anything other than trial mode. [Source: Mike Musgrove, *The Washington Post*, 26 Jan 2003] <http://www.washingtonpost.com/wp-dyn/articles/A40873-2003Jan24.html>

⚡ Spam continues to increase

Monty Solomon <monty@roscom.com>

Thu, 16 Jan 2003 22:38:57 -0500

The number of spam messages sent increased nearly 300 percent from 2001 to 2002 -- from 14,078,511 to 55,683,103, according to e-mail filtering company Brightmail. If you think you're getting more spam than ever, you're right. Spam has dramatically increased in the past year. And next year will be even worse. One new report says that by July, the volume of spam sent to business e-mail addresses will exceed the amount of regular e-mail.

[Source: *Newsfactor.com*, Janet Kornblum, 13 Jan 2003; PGN-ed]
<http://www.newsfactor.com/perl/story/20447.html>

✶ Canadian Centre for Identity Theft?

Richard Akerman <rakerman@bigfoot.com>
Wed, 15 Jan 2003 06:50:45 -0500

The National Archives of Canada already provide some Genealogy Research links and services

http://www.archives.ca/02/020202_e.html

They are polling, as part of the Canadian Genealogy Centre initiative

<http://cgc-ccg.archives.ca/>

Earlier poll results have been released

<http://www.globeandmail.com/servlet/ArticleNews/PEstory/TGAM/20030106/UFAMIO>

Q/national/national/national_temp/3/3/14/

<http://www.canada.com/ottawa/story.asp?id=%7B64AA74C1-25C8-415A-8574-5EA649947708%7D>

"Exactly half of those surveyed said they were either very interested (21 per cent) or somewhat interested (29 per cent) in being able to search for all Canadian genealogical information on a single Internet site."

Considering that most online and telephone credit card security consists of "shared secrets" such as: your name, address, phone number plus date of birth and mother's maiden name, this new Centre would seem to be an identity thief's paradise.

Just to make things even easier, the current Archives Genealogy FAQ points people at telephone directories, which can fill in the name-phone-address triplet:

http://www.archives.ca/02/02020201_e.html#8

I don't see that any consideration of this risk has been taken into account.

⚡ NASTAR web site provides personal skier information to anyone

"Robert H'obbes' Zakon" <Robert@Zakon.org>
Thu, 16 Jan 2003 13:56:44 -0500

NASTAR, the largest organization tracking amateur and professional ski races, is kind enough to post race results on its web site. You can

even search for a
ski racer by name.

By clicking on the ski racer's name, you get a page stating "I
am <ski racer
name> and I would like to login! [Click Here]". If the skier
has not done so
before (and most probably don't even know about it), you are
prompted to
create a password, and can then access a page containing the
racer's full
home address and birth date!

Seeing as NASTAR tracks not only professional racers, but
amateur and community
racers as well, they have quite an extensive database of
individuals.

After noticing the above behavior during last year's ski season,
I e-mailed
NASTAR and notified the local ski resort I race at. Of course I
never heard
back from NASTAR, and could only hope their system would have
been fixed for

And I thought I just had to look out for trees... No such luck
though.

✶ Re: Hard-coded calendar dates

John Sullivan <john.sullivan@thermoteknix.co.uk>
Mon, 6 Jan 2003 14:46:45 +0000

It's OK now though - they've fixed the JavaScript to read:

```
document.write(dayNames[day] + ", " + monthNames[month] + "  
" + date + ", 2003");
```

I'm stunned. There are just so many things wrong with this.

First of all I can't see any benefit to using a client generated date string anyway - why not just get the server to fill it in - one assumes amongst other things the server's clock is going to be more reliable than any random client's, plus I think it really should be tied to the time of the last update rather than whatever time it happens to be read at.

Second, the code immediately preceding initialises a variable called year - why, if they're just going to hard code the year as a string anyway? I suspect they had trouble deciding whether to add 1900 to the number returned from getYear or not. JS treatment of this varies between browser versions, and support for the improved getFullYear method may be patchy, but again a server filled date would solve this. (Actually, getFullYear is now sufficiently old for cross-browser support to be probably good enough.)

Thirdly, if you're doing it on the client, why not just use the Date object's own string formatting capability? The paper is English language only and none of the rest of the site is going to respond to the client's locale settings so I can see a stylistic point to fixing the date to the paper's own preferred format, but at least the Date object would get the year right without additional hackery.

🔥 REVIEW: "Internet Cryptography", Richard E. Smith

Rob Slade <rslade@sprint.ca>

Tue, 21 Jan 2003 08:14:34 -0800

BKINTCRP.RVW 20021215

"Internet Cryptography", Richard E. Smith, 1997, 0-201-92480-3,
U\$29.95/C\$44.95
%A Richard E. Smith internet-crypto@aw.com
%C P.O. Box 520, 26 Prince Andrew Place, Don Mills, Ontario
M3C 2T8
%D 1997
%G 0-201-92480-3
%I Addison-Wesley Publishing Co.
%O U\$29.95/C\$44.95 416-447-5101 fax: 416-443-0948 bkexpress@aw.
com
%O [http://www.amazon.com/exec/obidos/ASIN/0201924803/
robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/0201924803/robsladesinterne)
%P 356 p.
%T "Internet Cryptography"

According to the preface, this book is aimed at non-specialists who need to know just enough about cryptography to make informed technical decisions. As an example, Smith suggests systems administrators and managers who, while not formally charged with security, still have to use cryptographic techniques to secure their networks or transmissions.

Chapter one is an introduction, contrasting what we want; secure communications; with the environment we have to work in; a wide open Internet. The text also looks at the balance that must be maintained between convenience and requirements. Encryption basics, in chapter two, presents the concepts of symmetric cryptography, use, and choice. There is a clear explanation of the ideas without overwhelming technical details. (It is interesting to note how quickly the

cryptographic technology changes: SKIPJACK and ITAR were still important when the book was written, and are now basically irrelevant.) Some random thoughts on network implementation of encryption are given in chapter three. Managing secret keys, in chapter four, provides good conceptual coverage of generation and management, although the discussion of the problems of key escrow is weak. Because of the requirements for technical details when discussing protocols, chapter five, on IPsec, is different from other material in the book. It also includes a brief mention of other protocols. Chapter six discusses the use of IPsec in virtual private networks, while seven examines IPsec in terms of remote access. Chapter eight looks at IPsec in relation to firewalls, but it is difficult to see how this would be used in an actual application.

Chapter nine reviews public key encryption and SSL (Secure Sockets Layer). The basic concepts of asymmetric cryptography are presented well, but may be unconvincing due to the lack of mathematical support and details. While there is an introduction to the related idea of digital signatures, SSL is really only barely mentioned. World Wide Web transaction security, in chapter ten, provides practical examples of the technologies discussed. The same is true of email, in chapter eleven, but digital signatures get a bit more explanation. Chapter twelve builds on the signature concept to introduce PKI (Public Key Infrastructure) notions.

The fundamentals are written clearly and well, and are quite suitable for managers and users. Despite the lack of detail, the text may even be suitable for some security professionals who need a rough background without needing to work with the technology itself.

The work is easy to read, although the idiosyncratic structure may be confusing, and the value of some chapters questionable.

copyright Robert M. Slade, 2002 BKINTCRP.RVW 20021215

===== (quote inserted randomly by Pegasus Mailer)

rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

A fanatic is one who can't change his mind and won't change the subject. - Winston

Churchill

<http://victoria.tc.ca/techrev/~rslade> or <http://sun.soci.niu.edu/~rslade>

⚡ REVIEW: "Cryptography Decrypted", H. X. Mel/Doris Baker

Rob Slade <rslade@sprint.ca>

Wed, 22 Jan 2003 08:24:16 -0800

BKCRPDEC.RVW 20021215

"Cryptography Decrypted", H. X. Mel/Doris Baker, 2001, 0-201-61647-5,

U\$29.95/C\$44.95

%A H. X. Mel www.hxmelm.com

%A Doris Baker

%C P.O. Box 520, 26 Prince Andrew Place, Don Mills, Ontario
M3C 2T8

%D 2001

%G 0-201-61647-5

%I Addison-Wesley Publishing Co.

%O U\$29.95/C\$44.95 800-822-6339 fax 617-944-7273 bkexpress@aw.com

%O <http://www.amazon.com/exec/obidos/ASIN/0201616475/robsladesinterne>

%P 352 p.

%T "Cryptography Decrypted"

The book seems to be rather ambitious, since the preface says that it is addressed to any (and therefore all) audience(s), without any limitation on the stated purpose. In general, it is an attempt to portray the basic concepts of cryptography, without getting too far into technical details. Many other books have tried to do the same thing, and signally failed. Mel and Baker by and large succeed.

Part one addressed secret key (symmetric) cryptography. Chapter one tries to draw an analogy between locks and encryption, although the relation is strained at best. Substitution, frequency analysis, and polyalphabetic ciphers are covered in chapter two. Chapter three introduces transposition. The Polybius square is used, in chapter four, as an example of the combination of substitution and transposition. For those in the know, this leads nicely into the discussion of DES (Data Encryption Standard), in chapter five, although the neat segue would be lost on most readers, since the details of DES are not given. The history of cryptography appears rather abruptly in chapter six. Chapter seven covers the attempts to use cryptographic methods for confidentiality, integrity, authentication, and non-repudiation, and shows that the last point is not possible with purely symmetric cryptography. A simplistic examination of key exchange is given in chapter eight.

Part two deals with public key (asymmetric) encryption. Chapter nine is a confusing introduction using the Merkle puzzle space (with some mention of Diffie-Hellman) as the example. A simplistic review of

public key encryption is in chapter ten. Math tricks, in chapter eleven, seems pointless as it begins, but the development to the examples of modular inverses do provide both a basic form of asymmetric cryptography, and a demonstration of the mathematical concepts underlying more advanced cryptographic algorithms.

Chapter

twelve introduces authentication and digital signatures, with hashes

and message digests in chapter thirteen, and a discussion of digest

assurances (reviewing collisions and encrypted message authentication

codes) in fourteen. A comparison of cryptographic strength and speed

(between symmetric and asymmetric systems) is in chapter fifteen.

Part three covers the distribution of public keys, and introduces some

of the concepts of PKI (Public Key Infrastructure). Chapter sixteen

deals with certificates. The title of chapter seventeen relates to

the X.509 certificate structure, but the topics covered mostly concern

hierarchical certificate authorities. PGP (Pretty Good Privacy) and

the "Web of Trust" model are explained in chapter eighteen.

Part four looks at real world systems and actual applications.

Chapter nineteen explains email security, but in a generic fashion.

SSL (Secure Sockets Layer) is clearly described in chapter twenty,

but, given the lack of detail in the rest of the book, the technical

material is rather odd. IPsec, in chapter twenty one, is presented in

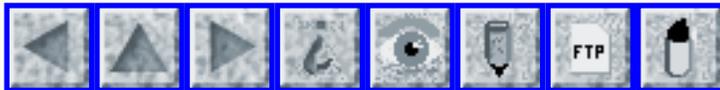
a confused manner. Various problems of, and attacks against, cryptography are outlined in chapter twenty two. The final chapter is

a simplistic review of the storage of cryptographic keys on smart cards.

This book does present most of the core concepts in cryptography. The text is readable, and, within the limited scope of the material, generally accurate. For non-specialists, it is a reasonable introduction to the topic. This might even include security professionals who are not directly involved with cryptographic systems. However, the lack of detail in the explanations of the theory is a weakness, since the text would be more convincing with more background.

copyright Robert M. Slade, 2002 BKCRPDEC.RVW 20021215
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

<http://victoria.tc.ca/techrev/~rslade> or <http://sun.soci.niu.edu/~rslade>



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

[ACM](#) Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 52

Monday 27 January 2003

Contents

- [Special notice to certain .MIL/.GOV subscribers](#)
[PGN](#)
- [Identity thefts doubled last year](#)
[NewsScan](#)
- [Crooks harvest bank details from Net kiosk](#)
[Fuzzy Gorilla](#)
- [Planned obsolescence of current games](#)
[Cody Boisclair](#)
- [Computer virus writer gets two years in prison](#)
[NewsScan](#)
- [SQL Slammer worm slows Net, grounds S.Korean surfers](#)
[Monty Solomon](#)
- [Bank of America ATMs hit by Slammer worm](#)
[Fuzzy Gorilla](#)
- [SQL Slammer: Are Admins really to blame?](#)
[Chris Leeson](#)
- [The worm turned back: Slammer damage contained](#)
[NewsScan](#)
- ['Slammer' Feared to Strike Again](#)
[Monty Solomon](#)

- [SQL Slammer in Canada](#)
[M Taylor](#)
 - [MS SQL Server worm info](#)
[Monty Solomon](#)
 - [Re: Keep it secret, stupid!](#)
[anonymous](#)
[Fred Cohen](#)
 - [Matt Blaze is a Hero](#)
[Robert Ellis Smith](#)
 - [Re: Trouble with Prime Numbers: DeCSS, DVD, ...](#)
[Bill Bumgarner](#)
 - [REVIEW: "Auditing Information Systems", Mario Piattini](#)
[Rob Slade](#)
 - [REVIEW: "Internet and Intranet Security Management", Lech Janczewski](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✉ **Special notice to certain .MIL/.GOV subscribers**

"Peter G. Neumann" <neumann@csl.sri.com>

Mon, 27 Jan 2003 14:07:03 PST

Dennis Rears will no longer be providing his very valuable .mil/.gov redistribution service. For many years, he has minimized the traffic flow from CSL to those domains, allowing me to send just ONE message for all of his subscribers. MANY THANKS to Dennis.

Those of you who were thusly subscribed have now been moved to CSL's majordomo server, as of this issue. This change may entail some new problems. Two people were unable to receive mail sent to a list, and I have given them individual one-of-a-kind subscriptions. Several

dozen people had addresses that bounced when sent from SRI. Some of those bounces were apparently already blacklisted even from Dennis's .mil site, and other bounces may be due to sites blocking RISKS from SRI as a result of overly aggressive spam filtering.

If you have friends and colleagues who complain that they are no longer getting RISKS, please show them this message, and suggest that they resubscribe at risks-request@CSL.sri.com. The majordomo server still has a few problems with its challenge-response mechanism, mostly due to upper/lower case incompatibility problems and also to certain noncompliant mailers. If you experience any difficulties, please let me know.

⚡ Identity thefts doubled last year

"NewsScan" <newsscan@newsscan.com>

Thu, 23 Jan 2003 08:40:35 -0700

The number of identity thefts doubled in 2002, with 162,000 reports of identity theft compared to 86,000 the previous year. However, the Federal Trade Commission says that the rise in identity theft complaints does not necessarily mean an increase in actual crimes -- it may simply reflect an increasing public awareness of the problem and a greater likelihood that such incidents are now being reported. But an official of the Michigan State Police points out that many former violent criminals are now using the

Internet for identity theft: "They are switching over to white-collar crime because it's more lucrative and they know they will get less time. Identity theft is not necessarily a sophisticated crime." [*The New York Times*, 23 Jan 2003; NewsScan Daily, 23 Jan 2003]
<http://partners.nytimes.com/2003/01/23/politics/23THEF.html>

🔥 Crooks harvest bank details from Net kiosk

"Fuzzy Gorilla" <fuzzygorilla@euroseek.com>
Mon, 27 Jan 2003 16:09:01 -0500

Crooks, operating in the Birmingham (England) area, are preying on people using public access terminals for Internet banking. The scam came to light after a *Register* reader discovered to his horror an authorised transfer of 6,300 pounds from the joint account he and his wife hold with Lloyds TSB. ...

"Lloyds have advised me that there is a large-scale Internet banking fraud taking place, affecting customers in the Birmingham area, and has been ongoing for several weeks. Apparently branches have been alerted," the victim, a company director of a West Midlands Net services firm, told us. "It appears that account details are being harvested from public access points (such as Internet Cafes, and more worryingly, Internet Kiosks)."

[Source: John Leyden, *The Register*, 27 Jan 2003; PGN-ed]
<http://212.100.234.54/content/6/29054.html>

✦ Planned obsolescence of current games (Re: Arrogance, [RISKS-22.46](#))

CodeMan38 <cody@zone38.net>

Sun, 26 Jan 2003 16:37:55 -0500

The "/Trivial/ Risks of Technical Arrogance" post in [RISKS-22.46](#) reminds me of a personal frustration, related to a game which *should* work on a recent operating system, but which, due to some apparent oversight by the programmers, simply refuses to run.

A certain popular video game, originally released on a rather failing console system but later re-released on the PC-- I won't mention it by name, but let's just say that its main character is a blue, spiny, fleet-footed anthropomorphic animal-- can even now be found in the discount racks of many software stores for \$10 US.

I bought this game before I upgraded to Windows XP; it was quite fun, and under Windows 98, it played exactly like the console version.

However, after I upgraded to XP, I discovered a sad truth about the game: it DOES NOT work on that operating system at all. Anywhere beyond the title screen, it causes a General Protection Fault in one of the old, obsolete DLLs used by the game, *even in the strictest compatibility mode that XP provides**. Technically, this is covered on the system requirements-- which

state "Windows 95/98"-- but there is nothing on the manufacturer's site mentioning an incompatibility with XP (something one generally wouldn't expect, given that every other Win98 game I've played works almost flawlessly in the new OS).

If the game in question were so-called abandonware -- that is, having gone out of production years ago -- I'd excuse it. But, as I mentioned, it can be found on store shelves at this very moment, and if I recall correctly, was also re-released in unaltered form either last year or the year before in a compilation.

And yet "Earthworm Jim", whose PC version was released even *earlier*, works absolutely fine in XP. Go figure...

✶ Computer virus writer gets two years in prison

"NewsScan" <newsscan@newsscan.com>
Fri, 24 Jan 2003 09:30:24 -0700

Simon Vallor, from Llandudno, Wales, was sentenced two years in prison by a London magistrate who said that Vallor's actions "cried out for the imposition of a deterrent sentence." The judge brushed aside Vallor's request for leniency, saying: "These offenses were planned and very deliberate. Frankly, when you go to this trouble to make a sophisticated virus, programmed to leave damage this week, next week and the week after,

it is absurd to claim you do not intend to do harm. These were by no means isolated offenses and they were committed over a period of time." Vallor wrote the viruses called Admirer, Redesi B, and Gokar, and was judged to be responsible wreaking damage in at least 46 countries. [*The Western Mail*, Wales, 22 Jan 2003; NewsScan Daily, 24 Jan 2003]
<http://shorl.com/hydragryhogrebro>

✦ SQL Slammer worm slows Net, grounds S.Korean surfers

Monty Solomon <monty@roscom.com>
Sat, 25 Jan 2003 12:27:33 -0500

A rapidly spreading computer worm infested networks and bogged down Internet traffic across the globe on Saturday, crippling online services in one of the world's most wired countries, South Korea. Called "Sapphire" or "SQL Slammer," the worm carries a self-regenerating mechanism that enables it to multiply quickly across the web, said Mikko Hypponen, manager of anti-virus research at F-Secure, a Helsinki-based computer security firm. [Source: Jane Macartney and Bernhard Warner, Reuters, 25 Jan 2003]

<http://finance.lycos.com/home/news/story.asp?story=31132872>

✦ Bank of America ATMs hit by Slammer worm

"Fuzzy Gorilla" <fuzzygorilla@euroseek.com>
Mon, 27 Jan 2003 16:07:10 -0500

The bandwidth-crunching Slammer worm caused all manner of damage since its appearance on the Net in the early hours of Saturday morning. The spread of the worm was so severe that the majority of Bank of America's 13,000 automatic teller machines "were unable to process customer transactions", according to **The Washington Post** -- which quotes the bank saying it was able to restore services on Saturday evening but a Seattle-based Reg reader tells us he was "unable to make a deposit to my Bank of America Account on Sunday at about noon Pacific time".

[**The Washington Post** article is not explicit about why the worm disrupted the ATM network. Whether the ATMs are attached to the Internet or whether the BoA server used by the ATM was infected, this does not sound very comforting.]

REFERENCES:

ATMs, ISPs hit by Slammer worm spread, by John Leyden, 27 Jan 2003

<http://www.theregister.co.uk/content/6/29054.html>

<http://www.washingtonpost.com/wp-dyn/articles/A43267-2003Jan25.html>

SQL Slammer: Are Admins really to blame?

"LEESON, Chris" <CHRIS.LEESON@london.sema.slb.com>

Mon, 27 Jan 2003 12:37:33 +0000

Over the weekend the SQL Slammer worm wreaked havoc across the Internet.

As usual the two most common responses are:

1. Blame Microsoft for producing code with holes in.
2. Blame the sysadmins for not patching systems.

[and 3. Nobody blames the anti-social [deleted] who wrote it]

Of course, (1) is a little unfair as Microsoft patched the hole six months ago. (2) seems to be a more reasonable response.

At risk of being flamed, I would like to suggest that it isn't.

We are frequently reminded in RISKS that we need to balance our viewpoint. There are risks in using technology, and risks in not using technology, and we need to accept that there is a tradeoff between the two.

This is a case in point. When a Service Update is applied to a system, a number of things are introduced:

- Bug Fixes
- New Bugs (due to changes in the system)
- New Code Behaviour (also due to changes in the system)

In theory, when a Service Update is applied to a computer, the Applications that are affected by the Service Release need to be re-tested to make sure that the Application still works correctly with the new level of the Operating System/DBMS.

Because Service Releases have such a wide scope this can be difficult in a development environment and near impossible in the live environment. In any case, testing takes time.

The requirement to maintain a "Stable Production Environment" may mean that

some Service Releases cannot be applied, regardless of what holes they fix.

This is not just a vague generalisation. I have seen systems I maintain brought down by DBMS Service Releases. There are also many examples that have appeared in the Risks Digest.

Our current system is held at a very old release because the next Service Release WILL break the application. This will require extensive work to find out all the places where code fixing is required.

Note that I am not saying that Service Releases should never be applied, I am saying that they should never be applied blindly.

🚀 The worm turned back: Slammer damage contained

"NewsScan" <newsscan@newsscan.com>

Mon, 27 Jan 2003 10:17:08 -0700

It's unlikely that there will be much additional destruction from the so-called Slammer computer worm that wreaked damage on the Internet over the weekend, by infecting more than a quarter of a million computer servers and clogging networks throughout the world. The worm targeted a known virus in Microsoft's 2000 SQL server database server; the company had issued software security patches in July 2002, but many network administrators had failed to install them. But now the worst appears to be over, says an executive at the security firm Symantec. [**USA Today**, 27 Jan 2003; NewsScan

Daily, 27 Jan
2003]

http://www.usatoday.com/tech/news/2003-01-26-networm_x.htm

'Slammer' Feared to Strike Again

Monty Solomon <monty@roscom.com>

Mon, 27 Jan 2003 14:23:10 -0500

'Slammer' Feared to Strike Again
Michelle Delio, Wired.com, 26 Jan 2003

The global worming attack that fried much of the Internet this weekend may return on Monday as unpatched systems and applications boot up at the start of the workweek. The worm can attack a multitude of Microsoft applications as well as applications distributed by other companies including administration, helpdesk, corporate antivirus and assorted security applications. Network administrators may not even be aware that their systems harbor programs that need to be patched. ...

<http://www.wired.com/news/infostructure/0,1377,57409,00.html>

SQL Slammer in Canada

M Taylor <mctaylor@privacy.nb.ca>

Mon, 27 Jan 2003 15:03:30 +0000

By one account, some Canadian government agencies were embarrassed to have

been caught off guard by the so-called SQL Slammer, a string of self-replicating computer code spread through data servers using Microsoft SQL [Server].

Royal Bank of Canada, Bank of Montreal and Canadian Imperial Bank of Commerce all reported virus-related glitches on Saturday. RBC's telephone and on-line banking systems were down for hours, and some CIBC and BMO cash machines worked sluggishly or not at all. Toronto-Dominion Bank also had problems but gave no details. Bank of Nova Scotia said its systems were unaffected.

[*The Globe and Mail*, 26 Jan 2003]

<http://www.globeandmail.com/servlet/ArticleNews/front/RTGAM/20030126/winterna>

M Taylor <http://www.mctaylor.com/>

MS SQL Server worm info

Monty Solomon <monty@roscom.com>

Sun, 26 Jan 2003 01:35:03 -0500

CERT Advisory CA-2003-04 MS-SQL Server Worm

<http://www.cert.org/advisories/CA-2003-04.html>

Cisco Security Advisory: MS SQL "Sapphire" Worm Mitigation Recommendations

<http://www.cisco.com/warp/public/707/cisco-sn-20030125-worm.shtml>

SQL Sapphire Worm Analysis

<http://www.eEye.com/html/Research/Flash/AL20030125.html>

Microsoft SQL Slammer Worm Propagation

<http://bvlive01.iss.net/issEn/delivery/xforce/alertdetail.jsp?oid=21824>

Unauthenticated Remote Compromise in MS SQL Server 2000

<http://www.nextgenss.com/advisories/mssql-udp.txt>

Sapphire SQL Worm Analysis

<http://www.techie.hopto.org/sqlworm.html>

Sapphire SQL Worm Scanner Tool

<http://www.eeye.com/html/Research/Tools/SapphireSQL.html>

Slammer slugs Internet, down but not out

<http://www.infoworld.com/articles/hn/xml/03/01/25/030125hnsqlnetupd.xml>

🔥 Re: Keep it secret, stupid! (Blaze, [RISKS-22.51](#))

<[name withheld by request]>

Mon, 27 Jan 2003

Matt Blaze has recently written (in <http://www.crypto.com/masterkey.html>

and <http://www.crypto.com/papers/mk.pdf>) about

his discovery of a vulnerability in master-keyed mechanical lock systems.

The paper is a well-written and detailed exposition of the technique, and

will serve well to educate readers both about the workings of mechanical

locks and about this particular attack. However, the attack may not be as

exciting and ground-breaking as claimed. For example, a friend and I figured

out how to do this in high school, but we realized that it would

be much more time-consuming and persnickety than other attacks that were practical in that environment. As for whether the attack uses "cryptanalytical techniques", that claim is hard to justify unless you consider "cryptanalytical" the most appropriate term for recursive exhaustive search.

It's hardly surprising that the technique is not widely covered in locksmithing texts. That's because it isn't particularly useful in legitimate contexts. No locksmith would ever bother going through all that rigmarole when he could instead disassemble the lock and read the master key directly--which is almost always possible if one has both a legitimate purpose and a legitimate key.

Given the generally low quality of original work in the underground community, I'm not very surprised that it's not well-known there, either. Most techniques I've gleaned from there have fairly clear origins in the adult world. That's not to say that execution by the underground isn't clever--but finding the 99th new buffer overflow in Internet Explorer is more a matter of persistence, I think, than it is of original thinking. After all, buffer overflows have been well-understood as a security flaw for over 30 years. The "MIT Guide to Lockpicking", for instance, is a clear and educational exposition of lockpicking, but doesn't present anything that hasn't been well-known in the locksmithing trade since before the invention of computers.

The basic vulnerability--that there are many more keys which will open the locks in a masterkeyed system than are ever actually delivered with such a system--IS well-understood and publicized to the trade. Locksmithing texts (some, at least) explicitly warn about deploying different masterkey systems in the same geographic area that use the same kind of keys, for that very reason. Lock manufacturers sell recommended keying patterns that are explicitly designed to avoid the problem, and I'm sure there is computer software that locksmiths use today for the same purpose.

A more interesting question is how to deduce the master key when you *don't* have a legitimate change key. That, too, is something we understood in high school, and it involves deducing patterns from several (temporarily) disassembled locks. Here, there's something resembling a genuine (although not especially difficult) cryptanalytical problem, in that one must deduce the pattern the lock manufacturer (or installer) used to assign the keys, and the manufacturer in turn can try to make that pattern difficult to deduce. That's the technique we used in actual practice, and it was an absorbing intellectual challenge at age 16.

The observation that customers aren't warned about this problem, well, that's hard to assess. One could make the same complaint about not warning customers that most mechanical locks can be picked in a few seconds. Fortunately, a lot of contexts where this is an issue (such as hotels) have already converted to different technologies that may be more

secure.

✶ Re: Keep it secret, stupid! (Blaze, [RISKS-22.51](#))

Fred Cohen <fc@all.net>

Sun, 26 Jan 2003 19:56:56 -0800 (PST)

When the original paper on Computer Viruses was sent to CACM for possible publication, they spent a year debating whether it should be considered for publication because of the potential harm that could be caused by people knowing about the vulnerability. I was so disgusted that I have not sent a paper to the ACM since that time.

Fred Cohen - <http://all.net/> - fc@all.net - fc@unhca.com

tel/fax: 1-925-454-0171 Fred Cohen & Associates - University of New Haven

✶ Matt Blaze is a Hero

"Robert Ellis Smith" <ellis84@rcn.com>

Mon, 27 Jan 2003 14:11:27 -0500

Congratulations to Matt Blaze for his extraordinary discovery about the vulnerability created by many master keys and especially for his forthright decision to publish his findings - after carefully weighing all of the consequences. The usual responses have been to keep findings like this a big

'secret' or to disclose the findings without any responsible planning or precautions. The critical messages he is receiving from the ostriches in the business are variations on a theme we have seen in other contexts. Matt tells it like it is, and he's a hero for doing so.

Robert Ellis Smith, Privacy Journal, PO Box 28577, Providence RI 02908
ellis84@rcn.com 401/274-7861 <http://www.privacyjournal.net> fax 401/274-4747

Re: Trouble with Prime Numbers: DeCSS, DVD, ... (Guadamuz, R-22.51)

Bill Bumgarner <bbum@codefab.com>
Mon, 27 Jan 2003 11:28:18 -0500

A slight clarification.

CSS-- the encryption used on DVDs-- was not designed to prevent the duplication of DVDs, illegal or otherwise. One can easily perform an 'image copy' of a DVD and the resulting copy will play just fine. On a Macintosh, it is trivial to create a disk image-- a virtual piece of media-- of any filesystem, including a DVD. The "virtual DVD" plays just fine and has the added advantage of lowering power usage on portable systems.

CSS is intended to prevent unlawful access to the content in three ways.

First, it makes it possible to enforce region codes in that it is [was]

impossible to decode the content without a licensed-- and likely region locked-- decoder. Region locking prevents a DVD targeted for the Japanese market from being played on a DVD player sold into the US market. The motivation behind this is to supposedly prevent cannibalization of sales between different units of large distribution companies. That is, Capital Records' US division does not want folks in the US purchasing something from Capital Records' UK division.

Second, it hinders direct lossless access to the contents of the DVD. This prevents folks from directly stealing the content and producing a derivative work. It also hinders digital to digital conversion to other, smaller, formats such as Video-CD (VCD's are hugely popular in the far East).

Finally, CSS provides a much greater degree of control over the distribution of content. This allows the content producers to tightly tune release cycles, marketing, etc.. to the business climate in a particular market. That is, they can charge what the market will bear in the target region. It also allows the media companies to control the production of the playback devices-- the content decoders. If you want to market and sell a DVD player, you have to buy a very expensive decryption key from the agency that controls CSS decryption keys [I believe it is the MPAA, but I'm not sure].

REVIEW: "Auditing Information Systems", Mario Piattini

Rob Slade <rslade@sprint.ca>

Fri, 10 Jan 2003 08:17:30 -0800

BKAUINSY.RVW 20020825

"Auditing Information Systems", Mario Piattini, 2000, 1-878-28975-6,
U\$139.95

%E Mario Piattini

%C 1331 E. Chocolate Ave., Hershey, PA 17033-1117

%D 2000

%G 1-878-28975-6

%I IRM Press/Idea Group

%O U\$139.95 717-533-8845 fax: 717-533-8661 cust@idea-group.com

%O [http://www.amazon.com/exec/obidos/ASIN/1878289756/
robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/1878289756/robsladesinterne)

%P 246 p.

%T "Auditing Information Systems"

Chapter one is a general overview of auditing, with few details. COBiT is not being used as intended by the majority of purchasers, we

are told in chapter two. There is a rather random discussion of some

security (and some network) concepts in chapter three, which changes

format rather abruptly towards the end. Chapter four notes that software maintenance has dangers and a structured process would help.

It also suggests a COBiT style list of objectives. All kinds of things it would be nice to have in the perfect data warehouse are described in chapter five. Chapter six looks at a few legal issues

with respect to information. The theme of chapter seven seems to be

that databases should do what they are supposed to. (I suppose Gene

Spafford could sympathize: his definition of a secure computer is one

that does what it is supposed to.) Chapter eight attempts to recreate ISO 9000 as a COBIT table. Task analysis by another name (audit function points) is described in chapter nine.

Even though the name of COBIT is repeatedly invoked in this book it is really hard to say what it has to do with auditing.

copyright Robert M. Slade, 2002 BKAUINSY.RVW 20020825
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

<http://victoria.tc.ca/techrev/~rslade> or <http://sun.soci.niu.edu/~rslade>

★ REVIEW: "Internet and Intranet Security Management", Lech Janczewski

Rob Slade <rslade@sprint.ca>
Thu, 9 Jan 2003 08:05:45 -0800

BKIISMRS.RVW 20020825

"Internet and Intranet Security Management", Lech Janczewski,
2000,

1-878-28971-3, U\$69.95

%E Lech Janczewski

%C 1331 E. Chocolate Ave., Hershey, PA 17033-1117

%D 2000

%G 1-878-28971-3

%I IRM Press/Idea Group

%O U\$69.95 800-345-432 fax: 717-533-8661 cust@idea-group.com

%O <http://www.amazon.com/exec/obidos/ASIN/1878289713/>

[robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/1878289713/robsladesinterne)

%P 302 p.

%T "Internet and Intranet Security Management: Risks and Solutions"

There is a heavy emphasis, in the preface, on the book's being up to date.

Yet the very first article relies on survey data that was three years old at the time the essay was written.

Part one supposedly talks about the state of the (security, one assumes)

art. Chapter one is a vague and superficial look at random topics and

technology related to security, plus results of the aforementioned opinion

poll. A list of Internet security problems, and solutions that are not

connected to the difficulties, make up chapter two.

Part two deals with managing Internet security. Chapter three has terse

descriptions of a number of theories of trust, related to some generic

security concepts. There are brief overviews of the TCSEC (Trusted Computer

System Evaluation Criteria), Common Criteria, and not-really-the-BS7799 in

chapter four. Out of thirty three pages in chapter five, three discuss the

general subject of Web security, while there is almost nothing on the

titular topic of management of Web security.

Part three reviews cryptographic and technical security standards. (There

are a great many grammatical errors, and the authors use almost-but-not-

quite standard terminology.) Chapter six is an opinionated piece, but does

touch on some basic cryptographic ideas. Myths and limitations of

cryptography are listed in chapter seven. Chapter eight has descriptions of

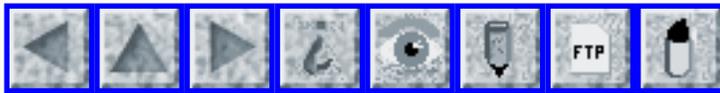
ISO cryptographic standards, both overly technical and incomplete.

Part four talks about law and security. Chapter nine discusses privacy, but only in regard to employer monitoring of employee email. The weaknesses of the New Zealand privacy law are commented on in chapter ten.

It is difficult to say that any audience would benefit from this vague collection of unfocused ideas.

copyright Robert M. Slade, 2002 BKIISMRS.RVW 20020825
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

<http://victoria.tc.ca/techrev> or <http://sun.soci.niu.edu/~rslade>



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 53

Thursday 30 January 2003

Contents

- [Berliner S-Bahn has computer trouble again](#)
[Debora Weber-Wulff](#)
- [Too much computing could give you a blood clot](#)
[NewsScan](#)
- [Microsoft, heal thyself!](#)
[NewsScan](#)
- [Slammer](#)
[PGN](#)
- [Interaction between SQL Slammer & furnaces](#)
[Jeremy Epstein](#)
- [Hacker insurance](#)
[NewsScan](#)
- [Pete Lindstrom's parametric worm warning](#)
[Jeremy Epstein](#)
- [12 U.Maryland students accused of high-tech cheating](#)
[Monty Solomon](#)
- [QUALCOMM Qsec-800 Secure CDMA phone](#)
[Monty Solomon](#)
- [Satellite system seen as a key life saver](#)
[Monty Solomon](#)

- [REVIEW: "Absolute PC Security and Privacy", Michael Miller](#)
[Rob Slade](#)
 - [REVIEW: "Information Security Best Practices", George L. Stefanek](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ Berliner S-Bahn has computer trouble again

Debora Weber-Wulff <weberwu@fhtw-berlin.de>

Wed, 22 Jan 2003 23:00:56 +0100

The worst problem since the last time....

RISKS readers will remember [RISKS-18.55](#) and [.60](#) in which the new Berlin light-rail switching computers had themselves a little glitch when they hit real service in 1998 -- a stack overflow.

Tagesspiegel (<http://archiv.tagesspiegel.de/archiv/12.01.2003/389362.asp>)

of 12 Jan 2003 reports that a little power-out at 13:35 the day before caused all three of the switching computers governing the track between Zoo and Ostbahnhof (the line with the most daily traffic, of course) to crash. It took until around 16:00 to get the systems back in service. Because this section of track is also in use by the Deutsche Bahn, many trains were terminated at stations outside of the city. Around 100 light-rail trainsets were stranded on open track. People were kept in the cars for up to 90 minutes. Luckily, the electricity came back on right away, so the heaters were on and people didn't have to freeze.

Those in charge have absolutely no explanation for the problem, etc. At least the fail-safe worked, and all the signals went to red. I suppose we have to be thankful for small blessings. Further reports just noted that there is no explanation for all of the computers (which are supposed to be on separate power lines) crashing at the same time.

I had hoped to be able to give more information, but the papers have dropped the topic in favor of more racy topics....

Prof. Dr. Debora Weber-Wulff, FHTW Berlin FB 4, Treskowallee 8, 10313 Berlin +49-30-5019-2320 <http://www.f4.fhtw-berlin.de/people/weberwu/>

⚡ Too much computing could give you a blood clot

"NewsScan" <newsscan@newsscan.com>
Thu, 30 Jan 2003 09:29:09 -0700

A research team in New Zealand has discovered a man who developed an almost-fatal blood clot after spending up to 18 hours a day at his computer workstation. The clot developed in his leg and traveled to his lungs.

Researcher Richard Beasley of the Medical Research Institute of New Zealand said that the problem could be widespread, and advised people who spend long periods using computers to stretch their legs frequently.

[*Globe News*/CNet New Zealand, 30 Jan 2003; NewsScan Daily, 30 January 2003]

<http://www.stuff.co.nz/stuff/0,2106,2226653a7144,00.html>

[... not to mention finger, hand, back, eye, and other problems. PGN]

Microsoft, heal thyself!

"NewsScan" <newsscan@newsscan.com>

Tue, 28 Jan 2003 08:30:32 -0700

Microsoft has been embarrassed by having to acknowledge that the SQL Slammer virus, which infected computer servers all over the world, also contaminated some of Microsoft's own servers, because system administrators had failed to heed the company's own advice to install a software patch months ago to fix a known system vulnerability. A Microsoft executive had to admit: "We, like the rest of the industry, struggle to get 100% compliance with our patch management. We recognize -- now more than ever -- that this is something we need to work on. And, like the rest of the industry, we're working to fix it." [*The New York Times*, 28 Jan 2003; NewsScan Daily, 28 January 2003]

<http://partners.nytimes.com/2003/01/28/technology/28SOFT.html>

Slammer

"Peter G. Neumann" <neumann@csl.sri.com>

Thu, 30 Jan 2003 12:27:42 PST

Of course, Microsoft's own SQL servers were victimized because they had not all been properly patched! Reports that the patches were available 6 months ago seem to be erroneous, because the patch for the Slammer exploit was apparently released only recently before the attacks. Although some folks are trying to put the blame on incompetent system administrators, I have heard that the service packs were poorly documented, and came in multiple versions depending on which SQL server software you were running, so that the SysAdmin burden was considerable. The worm affected many worldwide, including Bank of America's automatic teller machines, air-traffic control at Houston's Bush Intercontinental Airport, Cleveland, and New Jersey, American Express operations, and a Canadian Internet election.com vote in progress (which RISKS readers already know is not a great idea with respect to security). I had one out-of-band report that a major corporate research intranet was hosed because port 1434 accepted random UDP packets through the firewall.

And once again, the payload on this worm was relatively benign compared with the damage it could have done. The fact that so many different exploits keep recurring suggests that something is fundamentally wrong with the software development and operational processes. As I said at the Homeland Security Town Meeting panel in San Diego on 28 Jan 2003, the chickens of neglect are coming home to roost. The folks who should be developing sound

systems seem to have chickened out. Especially the non-bantam roost-ers who crow about their perfect security.

Interaction between SQL Slammer & furnaces

Jeremy Epstein <jeremy.epstein@webmethods.com>

Wed, 29 Jan 2003 11:55:42 -0800

With all the noise about SQL Slammer, I gave instructions on Monday to my staff to verify that all systems in our lab that run SQL Server were at the latest patch level. Not surprisingly, a few weren't, and so upgrades began. Several of the systems ended up dead, and we naturally blamed the patch install process, which is notoriously error prone.

In this case, though, there was another explanation. Midway through the install process, the fuses on one of the furnaces in the building blew (the outside temperature has been much below usual in Virginia for the past few weeks). This apparently sent enough of an electrical spike into the computers that we ended up with file system corruption in a way that wasn't resolved by an ordinary reboot, despite our UPSs & surge protectors. It also caused the temperature in the building to drop to a point where we were uncomfortable and having difficulty thinking carefully, especially given the obvious explanation of a failed patch. We don't quite know how it happened, but the file system corruption was both on Windows & Solaris boxes, so we're

sure it had nothing to do with the patch installation, and the electrical malfunction seems the most likely explanation.

The RISK is assuming that a system failure which occurs in temporal proximity to a security patch is in fact caused by the security patch!

Hacker insurance

"NewsScan" <newsscan@newsscan.com>
Wed, 29 Jan 2003 10:25:22 -0700

The latest cyber attack (last weekend's SQL Slammer virus, which infected thousands of computer servers throughout the world) has given a new boost to "network risk insurance" (AKA "hacker insurance"), which is expected to grow from the \$100 million industry it is now to a \$2.5 billion industry by 2005. Bruce Schneier, the chief technology officer for Internet security at Counterpane, thinks that insurance is every bit as important as prevention: "I believe that within a few years hacking insurance will be ubiquitous. The notion that you must rely on prevention is just as stupid as building a brick wall around your house. That notion is just wrong." But getting "hacker insurance" is not as easy as one might think, because insurers typically require a third-party assessment of the insurance applicant's security system, which might cost as much as \$50,000. [Reuters/
USA Today,

28 Jan 2003; NewsScan Daily, 29 Jan 2003]

<http://shorl.com/bupimybristumu>

✶ Pete Lindstrom's parametric worm warning

Jeremy Epstein <jeremy.epstein@webmethods.com>

Thu, 30 Jan 2003 10:07:53 -0800

[From Pete Lindstrom, Spire Security, petelind@spiresecurity.com]

<Adjective> Computer Worm <verb> Internet

In the wee hours of <date>, a <adjective> computer worm spread <adverb> throughout the Internet. Dubbed <silly name> because <ridiculous reason that doesn't explain anything about how it works>, and also known as <another random name> and <another random name>, the worm has infected an estimated <number> systems within <length of time>. Experts are calling this worm the most <adjective> since <date in the past>.

The worm exploits a hole in <Microsoft product name> that was first identified <number> months ago by <security company name>. In an attempt to secure the planet, <same company> released detailed information about the vulnerability and how to exploit it. They also mentioned how to fix it, but apparently <noun> listened. Coincidentally, the worm that exploited this hole was also first identified by <same company>. Even more coincidentally, they make a product to protect against <noun>.

"Actually, it's not really a <noun>, it's a <noun>," said <Pete Lindstrom, or some other person seeking publicity>. " A true <noun> works by <random filler that nobody will read>."

The worm's payload <verb> every system by <verb ending in -ing> the <noun>. Comparatively speaking, this is much worse than <another worm> but not as bad as <another worm>. The computers of <place> were hit the hardest. Current damage is estimated at <dollar figure more than the GNP of two-thirds of the world's nations>. " This worm has the potential to <something or other>," said <Pete Lindstrom, or some other person trying hard to come up with something interesting to say ;-)>. " It just goes to show you that <another something or other>."

Though there is no way to protect against this particular bug, experts recommend trying <longshot one> or <longshot two>, neither of which matter, since nobody will do it anyway.

★ 12 U.Maryland students accused of high-tech cheating

Monty Solomon <monty@roscom.com>
Sun, 26 Jan 2003 21:24:58 -0500

By Stephanie Hanes, Sun Staff, 26 Jan 2003

Twelve University of Maryland undergraduates have been accused of using Web-equipped cell phones or handheld organizers to cheat on a business

school final exam last month, according to the school's student-run Honor Council. Six of them have admitted to misconduct during that same test, the council said. The allegations prompted Provost William W. Destler to issue a warning to faculty members about the potential misuse of cell phones and other common handheld electronics, said J. Andrew Cantor, a 20-year-old senior and chairman of the Honor Council. ...

<http://www.sunspot.net/news/education/bal-md.cheating26jan26,0,3792093.story>

QUALCOMM Qsec-800 Secure CDMA phone

Monty Solomon <monty@roscom.com>

Wed, 29 Jan 2003 17:57:00 -0500

QUALCOMM's CDMA Technology Enhances Security Measures at Super Bowl XXXVII

Regional Homeland Security Agencies and Technology Partners Teamed Up To Provide Security Assistance for the Super Bowl -

SAN DIEGO, Jan. 29 /PRNewswire-FirstCall/ -- QUALCOMM Incorporated (NASDAQ:QCOM), pioneer and world leader of Code Division Multiple Access (CDMA) digital wireless technology, joined forces with regional homeland security agencies and technology partners to augment existing security measures for Super Bowl XXXVII. QUALCOMM, in partnership with the San Diego Regional Network on Homeland Security (RNHS) and other technology companies, assisted the San Diego Police Department

(SDPD) with security preparations for Super Bowl XXXVII by providing technology and products based on CDMA technology.

QUALCOMM provided wireless phones capable of carrying government-classified information over commercial cellular networks to federal law enforcement agencies and federal task force entities. These phones, referred to as the Qsec-800(R), are National Security Agency certified cellular phones developed through a U.S. Government contract with QUALCOMM. The phones represent a first step in securing the nation's cellular communications using the extensive CDMA network that is commercially available.

In addition to the secure wireless handsets, QUALCOMM had worked out an architecture that allowed the SDPD to access data, such as real time video as supplied by cameras, using digital technology from cVideo, at QUALCOMM Stadium, over commercial CDMA2000 1X networks. QUALCOMM's expertise in security ensured these data capabilities met the high standards set by the United States Department of Justice and local law enforcement. ...

<http://finance.lycos.com/home/news/story.asp?story=31220472>

✶ Satellite system seen as a key life saver

Monty Solomon <monty@roscom.com>

Mon, 27 Jan 2003 08:30:51 -0500

Tracking device crucial in rescues: Environmental satellites with

search-and-rescue tracking capability helped save 171 sailors, hikers, downed pilots, and others across the country last year, including 15 people in five incidents off the New England coast.

The Coast Guard requires all commercial fishing vessels and merchant ships to carry an Emergency Position Indicating Radio Beacon, which sends out a distress signal that NOAA satellites pick up and relay to the appropriate emergency response agency. Since it was launched in 1982, the satellite system is estimated to have saved 4,500 lives in the United States, said NOAA administrator Conrad C. Lautenbacher. ...

[Source: Jim Geraghty, States News Service, 26 Jan 2003; PGN-ed]

http://www.boston.com/dailyglobe2/026/nation/Satellite_system_seen_as_a_key_life_saver+.shtml

⚡ REVIEW: "Absolute PC Security and Privacy", Michael Miller

Rob Slade <rslade@sprint.ca>
Thu, 30 Jan 2003 08:05:48 -0800

BKAPCSPR.RVW 20021216

"Absolute PC Security and Privacy", Michael Miller, 2002,
0-7821-4127-7, U\$34.99/C\$55.95/UK#25.99

%A Michael Miller
%C 1151 Marina Village Parkway, Alameda, CA 94501
%D 2002
%G 0-7821-4127-7
%I Sybex Computer Books
%O U\$34.99/C\$55.95/UK#25.99 800-227-2346 info@sybex.com

%O [http://www.amazon.com/exec/obidos/ASIN/0782141277/
robladesinterne](http://www.amazon.com/exec/obidos/ASIN/0782141277/robladesinterne)

%P 530 p.

%T "Absolute PC Security and Privacy: Defend Your Computer
Against
Outside Intruders"

Miller never knew much about viruses, or took them seriously, until a friend got infected and it turned out to be more of a nuisance than he thought. So he decided to write a book about them. And also about spam, since he was annoyed by that, too.

Part one is about viruses, and other stuff. There are so many errors in the introduction, chapter one, that I don't know where to start. Since this book is obviously not written for professionals, is it important that it was Fred Cohen, and not Len Adleman, who did the first academic research on viruses? No. Is it important that the book constantly contradicts itself (for example, promoting the idea that virus writers are technically competent, and then pointing out that virus creation kits require no expertise at all)? Possibly not, but it doesn't inspire any confidence. Is it important that policies to prevent 95% of current viruses are dismissed in a single paragraph, buried in 150 pages of procedures (like the old "use only commercial software" myth--and the book also notes that commercial software has been distributed in an infected state) that might help protect you from some of the remaining 5%? Yeah, that could turn out to be significant. Chapter two talks about some high risk activities, but

the relevant points are hidden in a mass of relatively low peril particulars. Boot sector and file infectors are discussed in chapter three, but aren't important to users any more. Chapter four talks about macro viruses, but the suggested actions, such as manually deleting macros, are mostly ineffective. The material on script viruses, in chapter five, is quite confused: ActiveX is **not** a scripting system, and it is pushing the facts to say that Internet Explorer is a safe browser. (The procedures for disabling Windows Script Host could be useful.) The definitions, and particularly examples, of trojans, viruses, and worms are very confused in chapter six. Chapter seven examines e-mail and IRC (Internet Relay Chat) viruses, but concentrate on minor dangers and issues. Chapter eight warns against virus hoaxes, but does not tell how to identify them. The discussion of antiviral software in chapter nine deals **only** with scanning, and does not properly advise on limitations and weaknesses (such as the fact that real time, on-access, or firewall-based scanning may be 20% less effective than manual scanning). The other forms of antiviral software are mentioned in chapter ten, but so briefly as to be useless. "Preventing Virus Attacks," in chapter eleven, repeats earlier content. The suggested responses to a virus infestation, in chapter twelve, are seriously overblown.

Part two is concerned with Internet attacks. Given the preceding material, it is surprising that chapter thirteen provides reasonably good background on intrusion. But, given the tone and audience of the book, the attacks described are not relevant to the readership: most home users would not be able to do anything about the offensives described. The assaults listed in chapter fourteen are different, but

the mentions are too terse to provide any means of defence.

Chapter

fifteen suggests some good precautions, but does not explain the implications of following them. Chapter sixteen says that peer-to-

peer systems are dangerous, but is quite reserved given the level of

the threat and the scare tactics used elsewhere. Network protection

systems are briefly listed in chapter seventeen. "Choosing a Firewall," in chapter eighteen, describes the various types too poorly

for the user to make an informed choice. Chapter nineteen's advice on

dealing with an attack is too short to provide identification of a

real incident, and the response advice is unhelpful.

Part three supposedly deals with theft of privacy. Chapter twenty's

overview of threats against privacy is not bad, although it does confuse cookies, packet sniffing, and keystroke logging in the course

of a single paragraph. A discussion of online fraud, in chapter twenty one, is mostly about eBay, and mostly generic advice. A reasonable, if not extensive, set of explanations of harassment, spyware, and cookies are given in chapters twenty two, twenty three,

and twenty four, respectively. However, the background and suggestions in regard to passwords and encryption, in chapter twenty

five, are weak. The section finishes with anonymous surfing, in chapter twenty six.

Part four covers spam. Chapter twenty seven presents a good overview

of the basic concepts, but betrays a very weak technical understanding

of the subject. The recommended actions for protection and prevention

are not very effective. A more serious look at anti-spam activities

is in chapter twenty eight, but it boils down to a

recommendation not
to tell anyone your e-mail address: a suggestion that the book
itself
admits is not completely effective since spammers regularly
generate
random addresses to try. In addition, the information about
tracking
down and fighting against spammers is too brief to be of any use.
Chapter twenty nine recommends against forwarding chain letters,
but
probably should have more information about items such as the
technical impossibility of the messages that supposedly reward
you for
the number of missives you forward, and the variations on
"advance
fee" (aka "419" or "Nigerian scam") frauds.

It is unclear why "Web-Based Intrusions" could not have been
covered
elsewhere without creating a part five. Chapter thirty deals
sensibly
with pop-up ads, although I am not sure why disabling JavaScript
is
considered an extreme action, particularly in view of some of the
other recommendations in the book. The advice about the use of
the
hosts file, though, could be very helpful. Inappropriate
content and
filtering, in chapter thirty one, is handled rationally (if
curtly),
but does not mention the hidden agendas that filtering software
or
organizations may have.

Although some of the points in the book can be good, a great
deal of
the material is either too short to be really useful, or
questionable,
or wrong. In terms of security guides for the average user,
Crume's
"Inside Internet Security" (cf. BKININSC.RVW) is much better,
and so
is "Access Denied" (cf. BKACCDEN.RVW) by Cronkhite and

McCullough,
even though the latter is directed at managers.

copyright Robert M. Slade, 2002 BKAPCSPR.RVW 20021216
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

<http://victoria.tc.ca/techrev/~rslade> or <http://sun.soci.niu.edu/~rslade>

✶ REVIEW: "Information Security Best Practices", George L. Stefanek

Rob Slade <rslade@sprint.ca>
Wed, 29 Jan 2003 08:24:09 -0800

BKISBPBR.RVW 20021215

"Information Security Best Practices", George L. Stefanek, 2002,
1-878707-96-5

%A George L. Stefanek

%C 225 Wildwood Street, Woburn, MA 01801

%D 2002

%G 1-878707-96-5

%I Butterworth-Heinemann/CRC Press/Digital Press

%O 800-366-BOOK fax: 1-617-933-6333 dp-catalog@bh.com www.bh.com/bh/

%O <http://www.amazon.com/exec/obidos/ASIN/1878707965/robsladesinterne>

%P 194 p. + CD-ROM

%T "Information Security Best Practices: 205 Basic Rules"

The preface states that this book contains rules for a, possibly novice, system administrator and manager to provide a basic level of security for an organization.

Chapter one lists a few (well, eleven) attacks on information systems.

These are rather simple; the virus definition is quite old (there is no mention of macro or e-mail viruses) and worms are depicted in terms of memory exhaustion; and it is difficult to see what purpose they serve. The generic structure of an attack or intrusion is described in chapter two. The initial discussion of policy, in chapter three, is limited to the advice that you have one. This recommendation is expanded in chapter four, which does provide some reasonable points on creating a policy.

A few of the "rules" have been given in the earlier chapters, but chapter five, on network architecture and design, begins what is obviously the body of the book. Some of the advice is questionable, such as the commandment to limit firewall selection to those products that carry the NCSA stamp of approval. (The NCSA approval has some value, but is far from definitive, and, in any case, the group morphed into the ICSA many years ago, and is now TruSecure.) By and large the material, and that which follows, is reasonable and would help to improve the security of any enterprise, although it is quite limited.

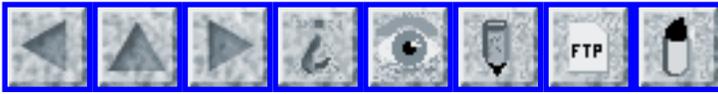
The remaining chapters cover physical security, PCs (tersely), Internet security, application development, software validation, configuration management, network monitoring, maintenance and troubleshooting, and training. The advice about hardware selection (in chapter six), is restricted to "motherhood" type rules which are vague and would be hard to follow. The chapters on network hardware (eight) and operating systems (nine) both recommend that there be a C2 level rating for routers and servers, although the "orange book"

specifications are no longer considered standards (and in spite of the fact that Windows NT 3.51 got a C2 rating--on condition that it was not connected to a network). Encryption, in chapter fourteen, is supposed to be "strong," although there is little information on how to measure strength. (In fact, a key length of 128 bits is mandated, despite the fact that this is far too short for asymmetric systems, and longer than triple DES [Data Encryption Standard].) The suggested actions in case of attack, in chapter nineteen, are rather drastic: spam should be addressed by killing e-mail service, and a denial of service attack should be responded to by disconnecting from the net.

Overall, this does have value as a "quick and dirty" set of guidelines for administrators who do not have formal security training and experience. The book is short, and thus easily readable for busy people. While security professionals may cringe at the simplistic nature of some recommendations, the rules can help improve the security of a system that would otherwise have none ... as long as the reader does not gain a false sense that he has implemented proper security.

copyright Robert M. Slade, 2002 BKISBPBR.RVW 20021215
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

<http://victoria.tc.ca/techrev/~rslade> or <http://sun.soci.niu.edu/~rslade>



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 54

Thursday 6 February 2003

Contents

- [Risks of all-electronic voting systems](#)
[David L. Dill](#)
- [NASA cultural failures on STS-107](#)
[Andrew Main](#)
- [Some very last Columbia data possibly rejected as "corrupted"](#)
[Eric De Mund](#)
- [Washington Monthly's 1980 critique of the space shuttle](#)
[Mike Godwin](#)
- [Astronauts may have the most dangerous job](#)
[Derek K. Miller](#)
- [All AA flights down due to computer crash](#)
[Keith Marzullo](#)
- [Air Canada "Jazz" airline grounded by computer glitch](#)
[Derek K. Miller](#)
- [19 charged in identity theft that netted \\$7 million in tax refunds](#)
[Benjamin Weiser via Monty Solomon](#)
- [Old data systems a health-care burden](#)
[Beth Healy via Monty Solomon](#)
- [Feds pull suspicious AONN.gov site](#)
[Declan McCullagh via Monty Solomon](#)

- [Spam filtering stops the democratic process...](#)
[David Wj Stringer-Calvert](#)
 - [SPAM from Microsoft](#)
[PGN](#)
 - [MS: Upgrade! HP: Don't upgrade!](#)
[Peter Kaiser](#)
 - [Caida analysis of the Sapphire worm](#)
[Colleen Shannon](#)
 - [Re: Trouble with Prime Numbers: DeCSS, DVD, ...](#)
[Bob Langford](#)
 - [REVIEW: "Cybercrime: Vandalizing the Information Society", Furnell](#)
[Rob Slade](#)
 - [Subject: REVIEW: "Cyberlaw: National and International Perspectives", Girasa](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ Risks of all-electronic voting systems

"David L. Dill" <elections@chicory.Stanford.EDU>
Sun, 02 Feb 2003 22:54:07 -0800

I am collecting endorsements for a statement I have written (with a lot of help) opposing electronic voting machines that do not produce paper ballots (or, in the future, some other independent voter-verifiable audit mechanism).

A lot of communities (and whole states, in some cases) are buying these machines because of pressure resulting from the 2000 election. The problem is that if errors or fraud are detected in an election using these machines, there is no way to recover, other than a revote. Worse, and more likely, errors or fraud may remain be undetected.

I have already collected endorsements from over 100 computer scientists, many of them leading experts in elections, computer security, and software engineering.

I have a Web page with background material, the statement, and the current list of endorsements. It would be great if you could join us in endorsing this statement. It would also be great if you could bring the issue to the attention of others who might be interested.

<http://verify.stanford.edu/evote.html>

If you are especially enthusiastic, other offers of help would be appreciated. This has turned out to be a bit more difficult than I thought it would be!

Thanks a lot, David Dill Stanford University

✶ NASA cultural failures on STS-107

Andrew Main <zefram@fysh.org>

Sun, 02 Feb 2003 22:16:58 +0000

On mission STS-107, the space shuttle Columbia (OV-102) suffered physical damage to its left wing during ascent. It is possible that this damage contributed to the subsequent breakup and loss of the orbiter during descent. During the entire flight, despite being aware that damage had occurred, NASA remained unaware of the extent of the damage,

making
inadequate efforts to determine the nature of the damage. This
error is
ascribed to three aspects of NASA's management of manned
spaceflights:
excessive reliance on checklists, cumbersome EVA procedures, and
a lack of
autonomy for astronauts in flight.

http://www.fysh.org/~zefram/nasa/sts107_culture.txt

[NASA is now backing off on the tile-damage theory. PGN]

✈ Some very last Columbia data possibly rejected as "corrupted"

Eric De Mund <ead@ixian.com>

Wed, 5 Feb 2003 22:42:47 -0800

When the Columbia shuttle stopped transmitting voice signals at
9 a.m, and
debris began raining down over a 200-mile-long swath of Texas
and Louisiana,
some data apparently continued to flow for another 32 seconds
after contact
was lost. However, computers on the ground rejected the data
because it was

"corrupted". NASA is trying to reconstruct this data. [Source:
John

M. Broder, NASA Now Doubts Tank Debris Doomed Columbia, PGN-ed]

*The New

York Times*, 5 Feb 2003; PGN-ed]

<http://www.nytimes.com/2003/02/06/national/nationalspecial/06XSHU.html>

One obvious solution would be to have at least one process save
all data,
corrupt or not.

Eric De Mund <ead@ixian.com> Ixian Systems, Inc., Mountain View,

CA

<http://www.ixian.com/ead/>

✶ Washington Monthly's 1980 critique of the space shuttle

Mike Godwin <mnemonic@well.com>

Mon, 3 Feb 2003 09:36:37 -0500

Washington Monthly has reposted its April 1980 critique of the space shuttle design. It's worth reading as a reminder that there have long been serious criticisms of the space shuttle for safety and economic reasons.

<http://www.washingtonmonthly.com/features/2001/8004.easterbrook-fulltext.html>

✶ Astronauts may have the most dangerous job

Derek K. Miller <dkmiller@pobox.com>

Wed, 05 Feb 2003 09:27:19 -0800

In an extreme example of computing risk, the December 1996 issue of Fast Company profiled the software developers for NASA's space shuttle program and tremendous rigour they apply to their jobs. Bill Pate, one of the senior programmers, is quoted: "If the software isn't perfect, some of the people we go to meetings with might die."

<http://www.fastcompany.com/online/06/writestuff.html>

The truth is, as we have been reminded, that might happen even if the software is perfect.

After the space shuttle Columbia broke up on re-entry last weekend, I wondered whether astronauts have the most dangerous job in (or around) the world. While I'm not a statistician, my quick calculations indicate that they do.

Fatality statistics are usually listed in numbers per 100,000, because for most activities they are pretty small: the risk of death is 2 per 100,000 scuba divers; 22 per 100,000 vehicle drivers; and 122 per 100,000 loggers (apparently the most dangerous of "normal" jobs).

We should be careful about making comparisons using astronauts and other occupations with very small numbers of participants, where we can only really calculate historical averages rather than yearly rates (which is how most fatality rates are reported).

With that in mind, however, I did a quick Google search and figured out that the death rate for astronauts and cosmonauts over the past 40+ years is (as of this week) about 7.5%, or 7,500 per 100,000 -- something like sixty times the rate for loggers. It is also nearly twice the 4.3% rate calculated for high-altitude mountaineering (often called the world's most dangerous job). That is especially notable since mountaineers often die from their own decisions, sometimes alone, while astronauts are supported by

thousands of people and billions of dollars in technology, but still die more frequently.

Other jobs have been more hazardous in the past. Sixty-three percent of German U-boat crew members were lost during World War II, nearly ten times the death rate of astronauts. But being a frontline soldier actively hunted in the open ocean during wartime is a different sort of "job," I would say.

I provide a bit more detail and links to my sources at:

http://www.penmachine.com/journal/2003_02_01_news_archive.html#90270862

with a followup here:

http://www.penmachine.com/journal/2003_02_01_news_archive.html#90276578

Again, these numbers are quick and off-the-cuff. But it seems pretty clear that being an astronaut has always been and will remain a very risky endeavour for the foreseeable future. Astronauts and cosmonauts have always known that very well, even if the rest of us sometimes forget.

Derek K. Miller, Vancouver, Canada dkmiller@pobox.com
Penmachine Media Company | <http://www.penmachine.com>

✈ All AA flights down due to computer crash

Keith Marzullo <marzullo@cs.ucsd.edu>
Thu, 30 Jan 2003 21:04:41 -0800

I was on a flight back from Chicago to San Diego yesterday afternoon. We

were scheduled to leave a bit after 5, but we instead took off around 6.

The pilot said that all American Airlines flights were unable to take off because "a big supercomputer in ... (I forget where; in the south, I believe) crashed." It seems, according to him, that all flight plans, weight allowances, and fuel amounts are computed at this one machine and distributed out to the flights.

I had not known of this single point of failure. Does anyone know more? How large of a region does this cover? Are crashes really rare enough to not have a hot standby? (Okay, AA is on the verge of bankruptcy).

✈ Air Canada "Jazz" airline grounded by computer glitch

"Derek K. Miller" <dkmiller@pobox.com>

Thu, 06 Feb 2003 09:34:30 -0800

A virus apparently attacked an AC Jazz flight-planning computer that provides essential information on fueling, weather, and other variables.

Without the computer's flight information releases, aircraft cannot take

off. The problem affected only Air Canada's regional operations. About 200

flights were affected, some canceled, some delayed. [Source: *National

Post*, 6 Feb 2003]

<http://www.nationalpost.com/national/story.html>

?id=%7B04638B16-6927-49FB-A548-1E8DC2D6E430%7D

✶ 19 charged in identity theft that netted \$7 million in tax refunds

Monty Solomon <monty@roscom.com>

Wed, 5 Feb 2003 22:23:39 -0500

Federal prosecutors in Manhattan have charged 19 people with being part of an identity-theft ring in the Bronx that received at least \$7 million in federal tax refunds by filing thousands of fraudulent income tax returns, using stolen Social Security numbers for people who were deceased or otherwise not filing returns. Having been implicated, one corrupt tax preparer in the Bronx then decided to cooperate with federal authorities, recording conversations and gathering evidence, and enabling the other culprits to be apprehended. (They used the IRS's electronic filing system!) The returns yielded an average of \$2500 each. [Source: Benjamin Weiser, **The New York Times**, 5 Feb 2003; PGN-ed]
<http://www.nytimes.com/2003/02/05/nyregion/05TAX.html>

✶ Old data systems a health-care burden

Monty Solomon <monty@roscom.com>

Tue, 4 Feb 2003 17:36:02 -0500

Handling bills, claims sends costs climbing

When President Bush took aim last week at bloated medical bills, he blamed lawyers, bureaucrats, and insurance companies for driving up costs. But

there is a hidden culprit he did not mention: woefully outdated back-office technology. The medical system has invested heavily in new ways to heal patients, but it has neglected the nuts-and-bolts business of managing bills and records. Of all the intractable challenges in health care, updating bill collecting and claims processing might seem the simplest to address. But the \$1.4 trillion health industry for years has lagged the rest of the economy in high-tech spending. Only agriculture and education spend less.

Even in Boston, where world-class hospitals spare no expense to treat cancer or deliver babies, and software gurus thrive on solving complex problems, health care was left behind in the drive for efficiency that changed the face of American business in the 1990s.

Dr. Harris A. Berman, chief executive of Tufts Health Plan, said the medical sector's failure to harness new systems is wasting a fortune: one-third of every health-care dollar is spent on administration. The piles of paperwork and thickets of mismatched databases make life more difficult for consumers and affect the care they receive. Bankers, car dealers, and tax collectors have all raced past health-care providers in basic technology, he said. ...

[Source: Beth Healy, *The Boston Daily Globe*, 4 Feb 2003]
http://www.boston.com/dailyglobe2/035/nation/Old_data_systems_a_health_care_burden+.shtml

⚡ Feds pull suspicious AONN.gov site

Monty Solomon <monty@roscom.com>

Wed, 5 Feb 2003 22:25:11 -0500

By Declan McCullagh

Staff Writer, CNET News.com

February 5, 2003, 4:00 AM PT

In a move that raises questions about the security of governmental domains, the Bush administration has pulled the plug on a .gov Web site pending an investigation into the authenticity of the organization that controlled it. Until recently, visitors to the AONN.gov Web site were treated to a smorgasbord of information about an agency calling itself the Access One Network Northwest (AONN), a self-described cyberwarfare unit claiming to employ more than 2,000 people and had the support of the U.S. Department of Defense. [HOWEVER,] no federal agency called AONN appears to exist, and no agency with that name is on the official list of organizations maintained by the U.S. National Institute of Standards and Technology. The General Services Administration (GSA), which runs the .gov registry, pulled the domain on Jan. 24, after a query from CNET News.com. ...

<http://news.com.com/2100-1023-983384.html>

[The entire message from Declan is at

<http://www.politechbot.com/p-04413.html>

A mirror of AONN.gov before it was taken down is at

<http://www.politechbot.com/docs/aonn/>

A subsequent message from Declan is at

<http://www.politechbot.com/>

as is information on how to subscribe. Wonderful stuff. PGN]

✶ Spam filtering stops the democratic process...

"David Wj Stringer-Calvert" <david.stringer-calvert@sri.com>

Wed, 05 Feb 2003 22:06:24 -0800

Rather ironically, Members of Parliament have installed an offensive-e-mail filtering system that overzealously blocked distribution of a Sexual Offences Bill as well as a Liberal Democrat consultation paper on censorship, among other things. [PGN-ed. No surprises there.]

<http://www.vnunet.com/News/1138508>

✶ SPAM from Microsoft

"Peter G. Neumann" <neumann@csl.sri.com>

Wed, 5 Feb 2003 13:31:34 PST

A colleague of mine just received this response from Microsoft, in response to a request to be REMOVED from an MS spam list. He/she remarked that "Not only is their SQL software buggy, it is slow too..."

Date: Wed, 5 Feb 2003 12:48:26 -0800 (PST)

From: Microsoft <TechEd2003@email.microsoft.com>

Subject: Don't miss TechEd 2003: The definitive Microsoft technology event ...

... Please note that it can take up to eight weeks to update customer

information in our database; therefore, you may receive e-mail from us within that time period.

⚡ MS: Upgrade! HP: Don't upgrade!

Peter Kaiser <kaiser@acm.org>

Sun, 02 Feb 2003 20:56:04 +0100

While searching the Hewlett-Packard site for information about a particular model of Presario 63xx computer (which, incidentally, appears unfindable through their usual mechanisms) I happened on

http://wss1pro.compaq.com/support/reference_library/viewdocument.asp?source=D0020926_CW01.xml&dt=3

Customer Advisory: D0020926_CW01 - Various Issues May Occur After

Installing Windows XP Service Pack 1 On Presario 6300 Series Computers

After installing Windows XP Service Pack 1 on Presario 6300 Series

computers and then performing a non-destructive restore, the system stops

responding and will not boot into Windows.... The user must perform a

destructive recovery to restore the system. All personal data that is not

backed up will be lost....

HP recommends that customers refrain from downloading and installing SP1

on Presario 6300 Series computers at this time.

"Various issues"! HP advises customers to "check back frequently", but the notice has been up for 4 months.

According to Microsoft, SP1 is an important upgrade:

Windows XP Service Pack 1 (SP1) provides the latest security and reliability updates to the Windows XP family of operating systems, and includes Internet Explorer 6 SP1. Windows XP SP1 is designed to ensure Windows XP platform compatibility with newly released software and hardware, and includes updates that resolve issues discovered by customers or by Microsoft's internal testing team.

The RISK to the normal user seems clear enough: the user may perform the upgrade without ever knowing about the "advisory" on HP's site. My brother, for whom I was doing the research, bought his computer after the date of the advisory, but had never heard about it; luckily I was able to warn him before he did anything foolish, like attempting to install this recommended upgrade.

✶ Caida analysis of the Sapphire worm

Colleen Shannon <cshannon@caida.org>

Fri, 31 Jan 2003 17:25:01 -0800

We have completed our preliminary analysis of the spread of the Sapphire/Slammer SQL worm. This worm required roughly 10 minutes to spread worldwide making it by far the fastest worm to date. In the

early stages

the worm was doubling in size every 8.5 seconds. At its peak, achieved approximately 3 minutes after it was released, Sapphire scanned the net at over 55 million IP addresses per second. It infected at least 75,000 victims and probably considerably more.

This remarkable speed, nearly two orders of magnitude faster than Code Red, was the result of a bandwidth-limited scanner. Since Sapphire didn't need to wait for responses, each copy could scan at the maximum rate that the processor and network bandwidth could support.

There were also two noteworthy bugs in the pseudo-random number generator that complicated our analysis and limited our ability to estimate the total infection but that did not slow the spread of the worm.

The full analysis is available at

<http://www.caida.org/analysis/security/sapphire/> (click on tech report)

<http://www.silicondefense.com/sapphire/>

<http://www.cs.berkeley.edu/~nweaver/sapphire/>

The animation (made by Ryan Koga and Jeffery Brown) is available at

<http://www.caida.org/analysis/security/sapphire/sapphire-2f-30m-2003-01-25.gif>

David Moore, CAIDA & UCSD CSE

Vern Paxson, ICIR & LBNL

Stefan Savage, UCSD CSE

Colleen Shannon, CAIDA

Stuart Staniford, Silicon Defense

Nicholas Weaver, Silicon Defense and UC Berkeley EECS

Caida mailing list <Caida@caida.org>

<http://login.caida.org/mailman/listinfo/caida>

[Re: Trouble with Prime Numbers: DeCSS, DVD, ... \(Bumgarner, R-22.52\)](#)

Bob Langford <langford@silicon-masters.com>

Thu, 30 Jan 2003 15:26:17 -0500

Bill Bumgarner's message in [Risks 22.52](#) clarifying the purposes of the CSS encryption used on DVDs is a clear, well-written statement of why CSS is used. However, there is one point on which I think he is mistaken. He said, "CSS is intended to prevent unlawful access to the content in three ways."

The problem here is the word "unlawful". These activities are not in themselves unlawful, although the MPAA would like everyone, including the legal system, to think that they are. These are activities the DVD publishers don't want you to be able to do, but with the exception of laws like the DMCA, they can only enforce their wishes by making it difficult. But to allow them to claim that they invented CSS to prevent "unlawful" activity makes a lot of otherwise fair uses of DVD appear illegal.

I was watching a movie the other day (Goldmember) that deactivated the fast forward, rewind, and pause buttons on my DVD player. The only way to watch it is from the beginning, without stopping. If the phone rings,

or
something else distracts you, too bad. You'll have to start the
movie over
to see what you missed.

Are the movie studios really wanting to claim it's unlawful to
watch this
movie any other way?

Bob Langford, Silicon Masters Consulting, Inc.

REVIEW: "Cybercrime: Vandalizing the Information Society", Furnell

Rob Slade <rslade@sprint.ca>
Thu, 6 Feb 2003 08:03:10 -0800

BKCYBCRM.RVW 20030121

"Cybercrime: Vandalizing the Information Society", Steven
Furnell,
2002, 0-201-72159-7, U\$29.99/C\$44.95
%A Steven Furnell
%C P.O. Box 520, 26 Prince Andrew Place, Don Mills, Ontario
M3C 2T8
%D 2002
%G 0-201-72159-7
%I Addison-Wesley Publishing Co.
%O U\$29.99/C\$44.95 416-447-5101 fax: 416-443-0948 bkexpress@aw.
com
%O [http://www.amazon.com/exec/obidos/ASIN/0201721597/
robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/0201721597/robsladesinterne)
%P 316 p.
%T "Cybercrime: Vandalizing the Information Society"

The preface states that this book is a general introduction to
cybercrime,
directed at any audience, and requiring no specific technical

background.

With certain provisos, those objectives are met.

Chapter one is a historical look at information and the rise of the net, dealing particularly with basic concepts and security. Computer related

crime is said to be happening, in chapter two, and some anecdotal examples

are given. Blackhat "celebrities" and groups are examined in chapter three.

While the jargon that Furnell uses tends to come from the media, his

research is obviously superior to that of many similar books on the topic.

Chapter four lists some exploits and attack approaches.

Malware, in chapter

five, also shows better than normal investigation, although some of the

terminology is dated. Societal aspects of cybercrime, in chapter six, seems

to rely primarily on opinion surveys, but there is some interesting material

on laws and the public perception of cybercriminals. Recent developments,

such as ethical hacking, hacktivism, information warfare, and cyberterrorism, are collected in chapter seven. Chapter eight lists some

recommended security practices.

The book does fall into the all-too-usual trap of concentrating on the

sensational side of information and network related crime (that of the

outside, and targeted, intruder), and therefore fails to provide a complete

picture. However, within its limits, the work does present a reasonable and

balanced view.

copyright, Robert M. Slade, 2003 BKCYBCRM.RVW 20030121
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

<http://victoria.tc.ca/techrev/~rslade>

or

<http://sun.soci.niu.edu/~rslade>

REVIEW: "Cyberlaw: National and International Perspectives", Girasa

Rob Slade <rslade@sprint.ca>

Mon, 20 Jan 2003 08:06:51 -0800

BKCBRLAW.RVW 20021126

"Cyberlaw: National and International Perspectives", Roy J. Girasa,

2002, 0-13-065564-3

%A Roy J. Girasa rgirasa@pace.edu www.prenhall.com/girasa

%C One Lake St., Upper Saddle River, NJ 07458

%D 2002

%G 0-13-065564-3

%I Prentice Hall

%O +1-201-236-7139 fax: +1-201-236-7131

%O <http://www.amazon.com/exec/obidos/ASIN/0130655643/>

[robsladesinterne](#)

%P 433 p.

%T "Cyberlaw: National and International Perspectives"

The back cover states that this is the "most comprehensive Internet law text for students of any discipline." The preface doesn't really contradict that statement, but then, it doesn't really specify a particular audience. The text itself, on the other hand, does not appear to be a reference, but rather a textbook for law students, and law students only. (American law students, at that.) While one cannot fault the author for the presumption of the publisher (who ultimately gets to decide on jacket copy),

the overly broad attempt at marketing is going to be frustrating for some readers.

Part one provides an introduction and examines jurisdiction. Chapter one is an introduction and overview of both the technology and law. This demonstrates a number of limitations (the technology is limited to the Internet), and, of course, the sort of bias one would expect to see in a legal text. (The definition of the Internet is taken from a "Finding of Fact" in the case that struck down the Communications Decency Act and contains a number of errors in terminology and, well, fact. The legal system is described only in terms of the various levels of US courts.) A number of cases regarding jurisdiction, first between US states and then between states and foreign States, is presented in chapter two. While this will undoubtedly be of value to US lawyers engaged in such battles, for the layman the best that can be determined is that a) the situation is indeterminate, and b) the material is confusing.

Part two deals with contracts, torts, and criminal law aspects of cyberspace. Chapter three looks at US case law regarding contracts and torts, including related topics such as commercial codes like UCITA. (Many implications of the legislation are poorly expressed: there are several paragraphs describing the implied warranties under UCITA, and a brief mention of the fact that using the words "as is" voids them all.) The construction of chapter four is very odd, since it begins with a review of

international statutes dealing with commercial online transactions, and then moves on to torts, and back to US cases. Although the first presentation of criminal cases is from Germany, all of the remaining material in chapter five, primarily on censorship, obscenity, and a little fraud, comes from the US.

Part three looks at intellectual property rights. Most of the copyright cases in chapter six, all from the US, deal with general issues unrelated to technology, at least not directly, while the cases presented in chapter seven are more directly related to technology. Chapter eight deals with trademarks, and the relation to technology is primarily made in terms of cybersquatting (the practice of registering a domain name using a famous name or trademark, so that the owner must buy it from you). Patents and trade secrets are covered in chapter nine, and the relation to network technology is rather slim.

Part four addresses privacy and security issues. Except that there is only chapter ten, on privacy.

Part five talks about antitrust, securities regulation, and relaxation. Antitrust, in chapter eleven, covers Microsoft, IBM, and a number of others. Chapter twelve's review of securities regulation cases primarily deals with fraud, and the technical links are basically irrelevant. The taxation of net businesses is in chapter thirteen.

As a textbook for law school students, this is undoubtedly

useful. The cases are collected, and questions are asked to encourage students to think about various aspects of cases, and related precedents that might be applicable. While US structures and law predominate, there is not only acknowledgement of foreign legislation, but some detailed case examination as well. In fact, practicing lawyers would also find this volume extremely valuable, for the direction in terms of case research on precedent if nothing else. For non-lawyers, such as security professionals, the content is extremely frustrating: all questions and no answers. Still, given the extremely murky state of US law in regard to the net and technology, this tome certainly could be worthwhile, even for those outside the US legal system.

copyright Robert M. Slade, 2002 BKCBRLAW.RVW 20021126
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

[ACM](#) Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 55

Weds 12 February 2003

Contents

- [Helsinki Health Department computer system down](#)
[Jesus Climent](#)
- [Hospital computer changes patient status from discharged to deceased](#)
[Steven Tepper](#)
- [Medical records: Turning lemons into lemonade or doublespeak?](#)
[Richard Cook](#)
- [Surplus computer in Kentucky held 'deleted' AIDS files](#)
[NewsScan](#)
- [TETRA radios pose some risk to hospital equipment](#)
[Martyn Thomas](#)
- [Boston artery errors cost over \\$1 billion](#)
[Monty Solomon](#)
- [TurboTax -- more security problems](#)
[Jim Garrison](#)
- [Stupid Security competition](#)
[Simon Davies](#)
- [Gambling on mobile devices? You bet!](#)
[Monty Solomon](#)
- [Senator Hagel of Nebraska ran his state's voting machines](#)
[Steven Hauser](#)

- [Judge suspends Washington State phone privacy](#)
[Monty Solomon](#)
 - [BC Student reprograms ID card, steals thousands](#)
[Steve Summit](#)
 - [Theft of disk drive at ISM Canada](#)
[Bruce Hamilton](#)
 - [Feds charge 17 with stealing satellite TV signals](#)
[Monty Solomon](#)
 - [Ex-hacker Mitnick's site vandalized](#)
[PGN](#)
 - [The non-paperless electronic office](#)
[Dick Mills](#)
 - [Password complexity](#)
[Jacob Palme](#)
 - [REVIEW: "PC Fear Factor", Alan Luber](#)
[Rob Slade](#)
 - [REVIEW: "Mastering Network Security", Chris Brenton/Cameron Hunt](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

🚨 Helsinki Health Department computer system down

Jesus Climent <jesus.climent@hispalinux.es>

Tue, 11 Feb 2003 13:36:17 +0100

A new data system named Pegasos has forced doctors in Helsinki to ask patients to remember their case history and to take hand notes. The fact that doctors cannot get any historical data forces them to spend more time writing (*sigh*) the data and reviewing the past treatments. As a conclusion, computers can, instead of speeding up the process, slow it down.

[Source: <http://www.helsinki-hs.net/news.asp?id=3D20030206IE8>]

Jesus Climent | Unix SysAdm | Helsinki, Finland | pumuki.
hispalinux.es

🔥 Hospital computer changes patient status from discharged to deceased

greep <greep@mindspring.com>
Wed, 12 Feb 2003 12:08:03 -0800

<http://www.baselinemag.com/article2/0,3959,880881,00.asp>

Eighty-five hundred people at St. Mary's Mercy [in Grand Rapids, Michigan] thought they were still alive. But the hospital's computers were telling them they were not.

...

It turns out St. Mary's Mercy had recently completed an upgrade of its patient-management software system... A "mapping error" in the conversion process resulted in the hospital assigning a disposition code of "20"--which meant expired--instead of "01," which meant the patient had been discharged.

Worse, that errant data wasn't sent just to the shocked patients but to their insurance companies as well as the local Social Security office, which helps determine whether elderly or disabled patients are eligible for Medicare. Obviously, once a patient is dead, Medicare--assuming its electronic-records system is accurate--isn't going to make any payments on bills for future medical

services or
medication.

✦ Medical records: Turning lemons into lemonade or doublespeak?

"Richard Cook" <ri-cook@uchicago.edu>

Mon, 10 Feb 2003 09:23:24 -0600

One remarkable aspect of techno-enthusiasm is the willingness to recast failure as a form of success. A long piece in CIO Magazine, "Off the Charts" describes a failure of the electronic medical record system as evidence of the value of the system itself. The piece describes a chip failure (burned out Alpha processor) that went on to generate a 20-minute delays in viewing medical records in the system at the University of Illinois medical center. According to the Christopher Koch, the author, the fact that "angry calls streamed into IS" from physicians (who had conveniently forgotten that there was a "read-only database that had been built for such emergencies") serves as prima facie evidence that the system is valuable. No mention is made of whether patient care was impeded or if missing information contributed to accidents during the interval. [http://www.cio.com/archive/020103/eva_charts_content.html]

If a small failure marks a favorable climate, perhaps a full fledged catastrophe marks real success?

Richard I. Cook, MD, Associate Professor Clinical Anesthesia and

Critical Care

Univ. Chicago, 5841 S. Maryland Ave MC4028, Chicago, IL 60637

www.ctlab.org

Surplus computer in Kentucky held 'deleted' AIDS files

"NewsScan" <newsscan@newsscan.com>

Mon, 10 Feb 2003 09:15:21 -0700

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;

NewsScan Daily, 10 February 2003]

http://www.usatoday.com/tech/news/2003-02-07-surplus-computer_x.htm

TETRA radios pose some risk to hospital equipment

"Martyn Thomas" <martyn@thomas-associates.co.uk>

Tue, 11 Feb 2003 09:59:58 -0000

The new TETRA two-way radio system is being widely adopted by emergency services. Because it is pulsed more slowly than GSM (17.6 Hz rather than 217 Hz) the signal is harder to filter and causes a greater level of RFI. For comparative tests on hospital equipment, see <http://www.medical-devices.gov.uk/mda/mdawebsitev2.nsf/webvwSearchResults/37CE5B0D2F6E45C900256A99005B8734?OPEN>

✶ Artery errors cost over \$1 billion

Monty Solomon <monty@roscom.com>

Sun, 9 Feb 2003 21:25:12 -0500

In the spring of 1997, David Beck of Bechtel/Parsons Brinckerhoff (the Big Dig's contracted managers) discovered that the entire 19,600-seat Fleet Center arena (whose own dig had begun in April 1993) was missing from the 1994 design drawings for what was then only a \$10.8-billion project. Instead, there was an obstacle-free area through which contractors were expected to lay utility lines. Bechtel apparently failed to fix the problem before signing off on the final design drawings three years later, which (according to the headline) cost over \$1 billion extra. [PGN-ed from Raphael Lewis & Sean P. Murphy, *The Boston Globe*, 9 Feb 2003, First of 3 articles.] http://www.boston.com/dailyglobe2/040/nation/Artery_errors_cost_over_1b+.shtml

✶ TurboTax -- more security problems (Re: [RISKS-22.51](#))

Jim Garrison <jhg@acm.org>

Thu, 06 Feb 2003 22:44:37 -0600

Apart from all the user uproar over TurboTax's activation scheme, the program has additional security problems. TurboTax's online registration and update facility will work only if Windows' Internet security parameters are reduced to their lowest setting (when you do this Windows itself tells you this setting is NOT recommended).

Access to online update is *required* because the distribution CDs are pressed before all tax forms are available and you **MUST** update the product in order to have the current forms for filing.

My Win2K system is on an internal LAN behind a Linux firewall, and Intuit tech support initially blamed the problems on this configuration. When I connected the Win2K system directly to the cable modem and reproduced the problem, they were forced to find the correct solution.

There are several RISKS here:

- 1) Telling people firewalls are a problem
- 2) Extremely poor error handling -- Both registration and online update just hang forever, displaying an "in progress" dialog box.
- 3) Writing code that requires the user to reduce Operating System security protections in order to use it.

✂ Stupid Security competition

Simon Davies <s.g.davies@lse.ac.uk>

Tue, 11 Feb 2003 02:19:35 +0000

PRIVACY INTERNATIONAL, MEDIA RELEASE
PRIVACY WATCHDOG LAUNCHES QUEST TO FIND THE
WORLD'S MOST STUPID SECURITY MEASURE

Global competition will identify absurd and pointless security requirements

The human rights watchdog Privacy International today launched a competition to discover the world's most pointless, intrusive, annoying and self-serving security measures. The "Stupid Security" award aims to highlight the absurdities of the security industry. Privacy International's director, Simon Davies, said his group had taken the initiative because of "innumerable" security initiatives around the world that had absolutely no genuine security benefit. "The situation has become ridiculous" said Mr Davies. "Security has become the smokescreen for incompetent and robotic managers the world over. I have stood for ages in a security line at an inconsequential office building and grilled relentlessly only to be given a security pass that a high school student could have faked. And I resent being forced to take off my shoes at an airport that can't even screen its luggage" he said.

Even before 9/11, a whole army of bumbling amateurs has taken it upon themselves to figure out pointless, annoying, intrusive,

illusory and just
plain stupid measures to "protect" our security.

It has become a global menace. From the nightclub in Berlin that demands the home address of its patrons, to the phone company in Britain that won't let anyone pay more than twenty pounds a month from a bank account, the world has become infested with bumptious administrators competing to hinder or harass us. And often for no good reason whatever.

Unworkable security laws and illusory security measures do nothing to help issues of real public concern. They only hinder the public and intrude unnecessary into our private lives.

Until 15 Mar 2003, Privacy International is calling for nominations to name and shame the worst offenders.

The competition will be judged by a panel of well-known security experts, public policy specialists, privacy advocates and journalists.

The competition is open to anyone. Nominations can be sent to stupidsecurity@privacy.org Winners will be announced on 3 Apr 2003 at the 13th Computers, Freedom & Privacy conference in New York.

✶ Gambling on mobile devices? You bet!

Monty Solomon <monty@roscom.com>

Mon, 10 Feb 2003 13:44:01 -0500

Because the newest cell phones are essentially mini-PCs, with full operating

systems, heavy-duty processor power, and high-resolution color screens, they are becoming better suited to remote gambling.

"Certainly wireless is the next generation of e-gaming that is looking to take hold," says Nancy Chan-Palmateer of CryptoLogic, a Toronto-based Internet gambling software company. The Internet gambling market is expected to bring in \$5 billion this year for casinos and game operators.

[Source: Chana R. Schoenberger, *Forbes*, 10 Feb 2003; PGN-ed]
http://www.forbes.com/2003/02/10/cz_cs_0210gaming.html

[Not surprisingly, this prompts your Moderator to note that today's all-electronic voting machines (without any voter-verified nonelectronic record of each vote) are essentially equivalent to Internet gambling on an unknown off-shore Web site. "Trust us. We're completely honest."
PGN]

✶ Senator Hagel of Nebraska ran his state's voting machines

Steven Hauser <hause011@tc.umn.edu>
Mon, 10 Feb 2003 10:54:00 -0600 (CST)

Republican Senator Hagel was the CEO of the company that produced the voting machines that tallied his "upset" victory in Nebraska. Go figure.

<http://www.thehill.com/news/012903/hagel.aspx>

<http://www.theregister.co.uk/content/55/29247.html>

Steven Hauser <http://www.tc.umn.edu/~hause011/>

[The machines used at the time were apparently a version of the AIS

DataMark mark-sense card system (now owned by ES&S) rather than all-electronic systems. PGN]

✶ Judge suspends Washington State phone privacy

Monty Solomon <monty@roscom.com>

Tue, 11 Feb 2003 12:36:10 -0500

AP Online, 11 Feb 2003

Washington state regulations to protect the privacy of telephone customer

account information, some of the toughest in the country, have been

suspended by a federal judge. State regulations that were adopted in

November [2002] and took effect in January [2003] required phone companies

to obtain customer approval before selling calling records or using them to

market anything but telecommunications services.

But Verizon Communications Inc. of New York, which has about 1 million

customers in Washington, sued the state, saying its Utilities and

Transportation Commission overstepped its authority and infringed on the

company's ability to speak to and serve customers.

U.S. District Judge Barbara J. Rothstein ruled Monday that Verizon had

raised "serious questions" about the constitutionality of Washington's

privacy rules, and granted a preliminary injunction blocking their

enforcement while the case is pending. ...

<http://finance.lycos.com/home/news/story.asp?story=31474529>

⚡ BC Student reprograms ID card, steals thousands

Steve Summit <scs@eskimo.com>

Fri, 07 Feb 2003 15:54:53 -0500

Like many colleges, Boston College has a multipurpose magstripe ID card which is used for identification, access, purchases at dining halls and the campus bookstore, and even local restaurants. A BC student managed to reprogram his ID card with the ID numbers of other students, meaning that he could purchase meals, textbooks, etc. with his charges showing up on the bills of others. Evidently he had (among other things) broken into the student center after hours and installed sniffing software on computers there so that he could obtain the information to reprogram his own card with. A spokesman reassures us that the BC system has been "upgraded to prevent future breaches".

http://digitalmass.boston.com/news/2003/02/07/bc_student.html .

The RISKS of these multi-use cards have been known for some time; see for example Andre DeHon's 1995 paper at <http://www.ai.mit.edu/people/andre/mit_card/security_assessment/security_assessment.html>.

It's reasonably interesting to see those fears being realized.

⚡ Theft of disk drive at ISM Canada

<bruce_hamilton@agilent.com>

Wed, 12 Feb 2003 09:17:34 -0800

Yesterday I received a letter which read, in part:

"Dear Valued Client,

"I am writing to inform you that on January 29, 2003, ISM Canada, a

subsidiary of IBM Canada Limited that provides client statement services

to Investors Group, notified us that a significant proportion of our

clients' 2002 third-quarter statement data was contained on a computer

hard drive that went missing from their Regina, Saskatchewan offices. Some

of our information was determined to be on the missing drive.

"I understand the concern this may cause for you. Investors Group wishes

to assure you that there is no ability for anyone to access your Investors

Group accounts with this information.

"The missing data is the same information that you see on your quarterly

client statement, being your name and address, your Investors Group

Consultant, the details of your Investors Group Plans and Accounts ... and

any beneficiary designations you may have made. The missing data *does not

include any of the confidential personal information typically involved in

the misuse of personal data,* such as social insurance numbers, dates of

birth, or banking information.

"IBM Canada and ISM Canada have expressed their regret to you and to

Investors Group, and have been working with us to ensure this matter is

handled quickly and properly. ISM had previously notified Investors Group

of a hard drive that was missing at the Regina facility, believed to

contain a small amount of securely protected Investors Group data. They

indicated that they were investigating the incident. Subsequently, on

January 29th, ISM Canada advised Investors Group of the full extent of the

missing data and that the local authorities were treating the incident as

a theft."

I checked my statement, and it's true that my SSN, DOB, etc., are not

there. I don't know what the author means by "banking information" since the

statement includes my name, account numbers, balances and previous quarter's

balances. This makes it much easier to do social engineering, e. g. "I notice

that my account #12345 is down 15%, so I'd like you to wire the remaining balance to ..."

The double reassurance that the data is "securely protected" and that it's

also not confidential is worrisome: if it truly were secure, we wouldn't

care whether it was confidential. I asked how the data was protected, and

haven't heard back yet. I *was* told that police have recovered the drive,

and the thief's apparent intention was to get the drive, rather than the data on it.

I'm curious about how somebody steals a disk drive from a presumably running system, but I'll be pesky about one question at a time.

bruce_hamilton@agilent.com Tel: +1 650 485 2818 Fax: +1 650 485 4917
Agilent Technologies MS 24M-A, 3500 Deer Creek Road, Palo Alto CA 94303

⚡ Feds charge 17 with stealing satellite TV signals

Monty Solomon <monty@roscom.com>
Wed, 12 Feb 2003 01:44:52 -0500

Seventeen people allegedly involved in the theft of satellite TV signals were arrested after a year-long undercover FBI investigation, as part of the FBI's nationwide "Operation Decrypt". Six of them were accused of violating the Digital Millennium Copyright Act, marking only the second grand jury indictment under that statute. Losses for satellite broadcasters reportedly involved millions of dollars. Source: Reuters, 11 Feb 2003; PGN-ed]

<http://finance.lycos.com/home/news/story.asp?story=31494999>

⚡ Ex-hacker Mitnick's site vandalized

"Peter G. Neumann" <neumann@csl.sri.com>
Tue, 11 Feb 2003 10:16:54 PST

Twice in the past two weeks, online vandals broke into the Web

server of
former hacker Kevin Mitnick's security start-up, Defensive
Thinking.

[Source: Robert Lemos, Special to ZDNet News, 11 Feb 2003]
<http://zdnet.com.com/2100-1105-984084.html>

[As one correspondent noted this item,
``As the credit card commercial says, 'Priceless.' ''

✶ The non-paperless electronic office

"Dick Mills" <dmills@mybizz.net>

Sun, 9 Feb 2003 17:54:24 -0500

My laptop shares a messy desktop with the usually assortment of
papers and
pencils. Yesterday I opened the CD tray, then shuffled around
the desktop
looking for the CD. I found it and was just about to close the
drawer when
I noticed that a staple had fallen into the CD tray.

Delicate electronics and paper do mix, sometimes not happily.

✶ Password complexity

Jacob Palme <jpalme@dsv.su.se>

Wed, 5 Feb 2003 00:32:00 +0100

Suppose you have an 8-digit decimal password. This means there
are 100
million possible combinations. You will on average need to try
on average 50
million times to find the right password by trial-and-error. Or,
if you have

the customary 3 tries before being forbidden access, the probability that you will get in by trial and error is $3/100\ 000\ 000$.

Suppose instead that you first have to pass one barrier with a 4-digit decimal password, and then pass a second barrier with a new 4-digit decimal password. You will then have to try on average 5 000 times on the first password, and then an average 5 000 time on the second password, or a total of on average 10 000 times. Or, if you have the customary 3 tries before being forbidden access in each step, you will have a probability of passing the first barrier of $3/10\ 000$ and then a probability of passing the second barrier of $3/10\ 000$. The probability of passing both barriers is then $9/100\ 000\ 000$.

In summary: The 8-digit barrier requires 5000 times more trials than the two 4-digit barriers to find the password, and the probability of success with the customary 3 allowed trials is three times higher with the two 4-digit passwords than with the single 8-digit password.

I gave this example as a comment on the debate of whether one strong security measure is better than several weaker, or the reverse.

Jacob Palme <jpalme@dsv.su.se> (Stockholm University and KTH)
for more info see URL: <http://www.dsv.su.se/jpalme/>

🔥 REVIEW: "PC Fear Factor", Alan Luber

Rob Slade <rslade@sprint.ca>

Fri, 31 Jan 2003 08:02:55 -0800

BKPCFRFC.RVW 20021219

"PC Fear Factor", Alan Luber, 2003, 0-7897-2825-7,
U\$24.99/C\$38.99/UK#17.99

%A Alan Luber www.alanluber.com

%C 201 W. 103rd Street, Indianapolis, IN 46290

%D 2003

%G 0-7897-2825-7

%I Macmillan Computer Publishing (MCP)

%O U\$24.99/C\$38.99/UK#17.99 800-858-7674 info@mcp.com

%O [http://www.amazon.com/exec/obidos/ASIN/0789728257/
robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/0789728257/robsladesinterne)

%P 362 p.

%T "PC Fear Factor: The Ultimate PC Disaster Prevention Guide"

The introduction states that the book is aimed at non-technical users, but doesn't further refine the purpose beyond saying that bad things happen to computers. We are also told that a system administrator is really a risk manager (which may come as a surprise to a number of sysadmins), and that if you read this book you will never have to worry about computer disasters again.

Even after reading chapter one I am not sure what the "root of all computer disasters" is, although I suppose that there is a fair chance that he means hard drives. There is a lot of irrelevant detail about the physical operations of drives, and Luber also is obviously confused between old hard drive crashes (caused when the heads physically contacted the platter, which was spinning at high speed) and modern "crashes," generally caused by bad pointers or other data errors. In chapter two, Luber

recommends, with opinions, but not much in the way of proof or backup, a bunch of software. Chapter three offers us more opinions, this time about buying a PC. Setting up a new PC is covered in chapter four. Most of chapter five prints documentation for a couple of antivirus programs and a firewall. A decent discussion of backup strategy, and more documentation of a backup program, is in chapter six. A manual for another backup program is in chapter seven. Restoring a backup comes in chapter eight. Chapter nine advises on maintenance. Some hoary old myths about risky activities (using shareware, for example) are recycled in chapter ten.

In one sense, Luber is right. If you keep your data backed up, you will be able to recover from pretty much any kind of disaster. On the other hand, I have said that in one sentence, and the book is over 300 pages long.

copyright Robert M. Slade, 2002 BKPCFRFC.RVW 20021219
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com
<http://victoria.tc.ca/techrev/~rslade> or <http://sun.soci.niu.edu/~rslade>

⚡ REVIEW: "Mastering Network Security", Chris Brenton/ Cameron Hunt

Rob Slade <rslade@sprint.ca>
Mon, 3 Feb 2003 08:19:32 -0800

BKMSNTSC.RVW 20021220

"Mastering Network Security", Chris Brenton/Cameron Hunt, 2003,
0-7821-4142-0, U\$49.99/C\$79.95/UK#37.99

%A Chris Brenton cbrenton@sover.net

%A Cameron Hunt cam@cameronhunt.com

%C 1151 Marina Village Parkway, Alameda, CA 94501

%D 2003

%G 0-7821-4142-0

%I Sybex Computer Books

%O U\$49.99/C\$79.95/UK#37.99 800-227-2346 info@sybex.com

%O <http://www.amazon.com/exec/obidos/ASIN/0782141420/>

[robsladesinterne](#)

%P 490 p.

%T "Mastering Network Security, Second Edition"

The introduction states that this book is aimed at systems administrators who are not security experts, but have some responsibility for ensuring the integrity of their systems. That would seem to cover most sysadmins. However, whether the material in this work is at a suitable level for most sysadmins is open to question. Now, to be fair to the authors, it seems that this second edition is a reissue, only marginally revised, of a book that was originally published seven years ago. (Under most standard contracts, publishers have the right to do this, and authors can't do much about it.) At that point, the material might have been pretty reasonable. Currently, it isn't.

Chapter one discusses systems theory. While the application of the text to network and security management is reasonably obvious in hypothetical terms, it is not at all clear in regard to direct operation in the real world. (This is particularly true for those who are not security

professionals.)

The systems development life cycle (SDLC) is covered in chapter two and, again, while it is an important topic, the relation to security is not made manifest. The introduction to networking itself covers the OSI (Open Systems Interconnection) model, routing, and bits of TCP/IP, in chapter three. One would have thought that this would have been old news to sysadmins. The same is true of the material on transmission and network topology, in chapter four. There is some mention of security issues, but the discussion is minimal.

Chapter five has a reasonable overview of firewalls, although the terminology is not always standard. Chapter six is documentation for the Cisco PIX firewall. The information about intrusion detection systems, in chapter seven, provides good material on points often neglected by other works, and adds a guide to Snort. The coverage of cryptography, in chapter eight, has a confusing structure. Most of the material on virtual private networks consists of screen shots of Microsoft's RRAS (Routing and Remote Access Server), in chapter nine.

Chapter ten relies on old concepts and technologies to discuss viruses and other malware. Disaster prevention and recovery, in chapter eleven, concentrates on building redundancy and the VERITAS server based backup system. A good deal of information about Windows, most of which may have some relevance to security, is in chapter twelve. Some introductory, and some network, data about UNIX is available in chapter thirteen.

Chapter

fourteen describes how information can be obtained about your system in order to mount an intrusion attack. Some resources for security are mentioned in chapter fifteen.

Overall, the book does provide a fair amount of information that would likely be of help to most network administrators in securing their systems and networks. However, there is also a lot of detail that is not directly relevant to the task, some erroneous content, and not a few gaps. While the original authors may have mastered their topic, the volume currently on offer does not reflect that.

copyright Robert M. Slade, 2002 BKMSNTSC.RVW 20021220
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

<http://victoria.tc.ca/techrev> or <http://sun.soci.niu.edu/~rslade>



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 56

Tuesday 18 February 2003

Contents

- [Identity theft evidently based on spoofing AOL](#)
[Mike Hogsett](#)
- [Credit-card hacking](#)
[David Wj Stringer-Calvert](#)
- [11-year-old boy charged with felony for computer tampering](#)
[David R. Throop](#)
- [eBay Sting](#)
[D. Joseph Creighton](#)
- [Edsger Dijkstra quote on Computer Science](#)
[Stan Mazor](#)
- [MacOS 10.2.4 update & httpd.conf replacement](#)
[Lawrence Brenninkmeyer](#)
- [Risks of Doing Homework](#)
[Rebecca Mercuri](#)
- [Re: Hospital claims 8,500 people expired](#)
[Fredric L. Rice](#)
- [Re: Artery errors cost over \\$1 billion](#)
[Jamie McCarthy](#)
- [Re: Password complexity](#)
[Nick Brown](#)

- [Questions Frequently Asked About Rob Slade's Innumerable Book Reviews](#)
[Rob Slade](#)
 - [REVIEW: "Honeypots: Tracking Hackers", Lance Spitzner](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ Identity theft evidently based on spoofing AOL

Mike Hogsett <hogsett@csl.sri.com>

Tue, 18 Feb 2003 15:49:02 -0800

A Web site, <http://www.aol-billsite.com/>, was recently brought to my attention. It has questionable content and most certainly a questionable intent. From my investigation, it appears that the intent is to purloin the information necessary for identity theft from unsuspecting AOL subscribers.

In summary, the domain name www.aol-billsite.com serves a web page that uses a frame set to obscure the source of the real contents. The real contents contain a very official looking form for "customers" to enter new billing information for their AOL account. In addition to a credit-card number this form asks for social security number, mother's maiden name, and a second credit-card number.

If some poor, unsuspecting person actually presses the submit button on this page, the information is sent in the clear to a CGI program on yet another web server which presumably sends this information via e-mail (also in the

clear) to a hotmail.com e-mail account.

I believe it is immediately evident that the intention is to steal the information necessary to perform identity theft.

Why don't I believe that it is not an official AOL page?

- 1) Original frameset page not served via https
- 2) Obfuscation of true source of content
- 3) Content not served via https
- 4) Form contents not sent via https to form target
- 5) Form contents sent to form target on third web server in yet another domain
- 6) hotmail.com address given as argument to form target
- 7) Real page server via a residential broadband address
- 8) Form asks for home address, date of birth, SSN, mother's maiden name,
and a second credit-card number
- 9) Form asks for AOL password
- 10) Two of the relevant domains registered by individuals
- 11) Domain/host information spans the US (WA to CA to NJ to FL)
- 12) Form contents e-mail is sent via a completely insecure CGI program
(anyone can send e-mail anywhere with this script).

[Update: The abuse@hotmail.com auto-responder rejected my report, for the following ERRONEOUS reason! (My e-mail has numerous references to hotmail.) Mike

"Unfortunately, we cannot take action on the mail you sent us because it does not reference a Hotmail account. Please send us another message that contains the full Hotmail e-mail address and the full e-mail message to:
abuse@hotmail.com "
]

[If it this case is due to stupidity and ignorance rather than an

outright scam, that would be even more startling -- although the opportunities for privacy violations would still be enormous. Furthermore, the recipient mailbox is reportedly saturated, which suggests perhaps that people are incredibly gullible and have already bitten for this scam! Also commented on by Fred Gilham. PGN]

✶ Credit-card hacking

"David Wj Stringer-Calvert" <david.stringer-calvert@sri.com>
Tue, 18 Feb 2003 07:33:28 -0800

More than five million Visa and MasterCard accounts throughout the U.S. were accessed after the computer system at an unidentified third-party merchants' processor was hacked into. It is currently believed that no fraudulent misuse has occurred. MasterCard began to notify its financial members during the week of 3 Feb that more than 2 million MasterCard accounts had been potentially compromised -- as did Visa for about 3.4 million of its accounts. [Source: Reuters item, 18 Feb 2003; PGN-ed]

http://story.news.yahoo.com/news?tmpl=story2&cid=581&ncid=581&e=10&u=/nm/20030218/tc_nm/financial_visamastercard_dc

✶ 11-year-old boy charged with felony for computer tampering

David R. Throop <throop@cs.utexas.edu>

13 Feb 2003 23:01:58 -0600

A St. Lucie West Middle sixth-grader used the excuse of forgetting his lunch to return to his reading classroom and sat down at his teacher's computer to change five reading assignment grades, St. Lucie County sheriff's deputies said Tuesday. ... The 11-year-old student, who faces a 10-day suspension and a principal's recommendation that he be expelled, was arrested Monday on a felony charge of offense against intellectual property. ... The student was booked into the St. Lucie County jail, then released to his father. Mancini said he could face several years in a juvenile detention facility, if convicted.

http://www.gopbi.com/partners/pbpost/epaper/editions/wednesday/martin_stlucie_e394fc8032005260000b.html

[With a little more imagination, he could have qualified for life imprisonment under the new anti-hacking law. PGN]

eBay Sting

"D. Joseph Creighton" <djc@cc.UManitoba.CA>

Tue, 18 Feb 2003 14:54:19 -0600

A computer technician in Winnipeg, Canada, had his Fluke inline network tester stolen (approx. value CDN\$11,000) at the end of January. Later,

he decided to check if the not-so-common device was being put up for sale on eBay and found two: one in Indianapolis and the other in Winnipeg.

[First source: CBC Radio with an online article:
<http://winnipeg.cbc.ca/template/servlet/View?filename=mb_ebay20030218>]

After expressing interest and through correspondence with the seller, a serial number was obtained which confirmed that the network tester was the technician's. Police were contacted and a meeting was arranged at a local coffee shop where the seller/suspect was arrested. *The Winnipeg Free Press* for 18 Feb 2003 later mentioned that the meeting between seller and technician occurred with two plainclothes officers waiting at another table.

[I presume the police were drinking Tester's Choice with their serial. PGN]

It appears the CBC may have gotten their tip from the morning paper -- I don't get to my own copy until the end of the day -- and there's a bit of a difference between the radio and newspaper versions.

Although the suspect may be innocent of the theft, the attempt to sell would seem to constitute a crime. The RISKS in not doing your on-line research before doing your on-line auction is -- for the seller -- one that might be costly and -- for the thief -- downright dumb.

D. Joseph Creighton [ESTP] | Systems Analyst, Database Technologies, IST
Joe_Creighton@UManitoba.CA | University of Manitoba Winnipeg, MB, Canada, eh?

✶ Edsger Dijkstra quote on Computer Science

Stan Mazor <smazor@numeritech.com>

Mon, 10 Feb 2003 09:55:17 -0800

[From asilomar-news, noted by Robert G. Kennedy III in Hackers newsgroup,
sent to RISKS by Ken Knowlton. PGN]

Edsger W. Dijkstra, *Communications of the ACM*, Mar 2001,
Vol. 44, No. 3

In academia, in industry, and in the commercial world, there is a
widespread belief that computing science as such has been all
but
completed and that, consequently, computing has matured from a
theoretical
topic for the scientists to a practical issue for the
engineers, the
managers, and the entrepreneurs. [...]

I would therefore like to posit that computing's central
challenge, "How
not to make a mess of it," has not been met. On the contrary,
most of our
systems are much more complicated than can be considered
healthy, and are
too messy and chaotic to be used in comfort and confidence.
The average
customer of the computing industry has been served so poorly
that he
expects his system to crash all the time, and we witness a
massive
worldwide distribution of bug-ridden software for which we
should be
deeply ashamed.

For us scientists it is very tempting to blame the lack of

education of

the average engineer, the shortsightedness of the managers,
and the malice

of the entrepreneurs for this sorry state of affairs, but that
won't

do. You see, while we all know that unmastered complexity is
at the root

of the misery, we do not know what degree of simplicity can be
obtained,

nor to what extent the intrinsic complexity of the whole
design has to

show up in the interfaces. We simply do not know yet the
limits of

disentanglement. We do not know yet whether intrinsic
intricacy can be

distinguished from accidental intricacy.

To put it bluntly, we simply do not know yet what we should be
talking

about, ... The moral is that whether computing science is
finished will

primarily depend on our courage and our imagination.

[Stanley Mazor, Director Customer Services, Numerical
Technologies Inc.

70 West Plumeria Drive, San Jose, CA 95134-2134 1-408-273-4485]

🔥 MacOS 10.2.4 update & httpd.conf replacement

Lawrence Brenninkmeyer <ldb@northwestern.edu>

Fri, 14 Feb 2003 10:56:43 -0600

The Mac OS X operating system is a work in progress. Users are
treated to

small upgrades every one or two months that fix bugs, improve
security, and

occasionally provide increased functionality. Presumably in an
effort to

add functionality to the built-in Apache server, the latest

update installs a brand new httpd.conf file. This is file that tells the Apache server how to configure itself (which modules to load, where the root directory is, etc.) The update kindly (and silently) saves the original httpd.conf as httpd.conf.applesaved. The risk is that replacing the original, not telling anyone, and then leaving the server active on restart can lead to a breach of security. One of the things that you can use the httpd.conf file for is to govern which directories are password protected and which are not [1]. This information is not retained in the new httpd.conf, so directories that were password protected are opened to the world after the update has been installed.

The risks are obvious, and so are the solutions. At a minimum, they should have disabled Apache on startup and presented the user with a dialog box informing them of the change.

[1] Apache httpd documentation: Basic Security
<<http://httpd.apache.org/docs/howto/auth.html#basic>>

<<http://pubweb.northwestern.edu/~ldb371/>>

✶ Risks of Doing Homework

"Rebecca Mercuri" <notable@mindspring.com>
Thu, 13 Feb 2003 05:46:37 -0500

At the faculty meeting at Bryn Mawr College on 12 Feb 2003, we

were informed that a student at Haverford (our affiliated College) was arrested over the weekend when he was trying to do his homework assignment in Philadelphia. As part of the Cities project, he was taking photographs of SEPTA (our regional transit authority) facilities when he was arrested, detained for a few hours, and eventually released. Haverford administration is working to try to ensure that this event not be a part of the student's permanent police record. Apparently taking photographs at transit facilities is cause for arrest during "Code Orange" alert, the authorities explained. Faculty were advised to be careful about assigning "field trip" projects during such alerts.

Rebecca Mercuri, Bryn Mawr Computer Science

✶ Re: Hospital claims 8,500 people expired

"Fredric L. Rice" <Quack@SkepticTank.ORG>

Thu, 13 Feb 2003 11:18:28 -0800

In [RISKS-22.55](#), the coverage of the hospital in Grand Rapids, Michigan didn't mention the possibility of *deliberate* abuse of the system where simply changing a 01 into a 20 causes the system to inform insurance carriers, the IRS, and presumably other agencies that one's dead. Since a hospital is a credible source for agencies, someone trying to vanish in

I have absolutely no training in probability theory, but it seems to me intuitive that adding a mechanism that effectively tells you if you're already half-right, is going to reduce the security of any password.

Consider an eight-digit combination lock versus two four-digit locks, where the first four-digit lock goes "click" before you open it and move on to the next. Clearly you only have to go round the 10000 combinations of the second lock once, whereas in the 8-digit lock, you might have to do it 10000 times. Or to make it even clearer, consider eight one-digit locks.

The calculation of the relative ease of cracking the combination only becomes non-trivial when the number of bits in the separate locks sums to more than the number of bits in the single lock.

However, as long as the main limiting factor in determining the minimum length of a password for, say, an online banking system, is the marketing department ("Oh, no, we mustn't frighten the customer with a hard-to-remember code; let's use four digits like for the ATM card. But don't forget to insist on a 128-bit browser, because the user wants to feel safe."), the debate will remain academic anyway. :-)

[Similar comments were received from Simon Waters and David Parnas.

Of course, one of the CLASSIC password attacks was the old TENEX flaw in which passwords were checked one character at a time. By aligning the password presented in a program so that the NEXT character lay

across a

page boundary, you could detect whether or not a page fault had occurred

on the previous character, and thus iteratively reduce an exhaustive

search to a linear search. This was something like 30 years ago when

it was realized that visibility of intermediate results is riskful, and

that checking must be done in a single atomic transaction.
PGN]

✶ Questions Frequently Asked About Rob Slade's Innumerable Book Reviews

Rob Slade <rslade@sprint.ca>

Thu, 13 Feb 2003 16:38:22 -0800

OK, since I am now getting not only questions about the reviews every day, but

multiple copies of the **same** questions, I suppose it is time for:

Questions Frequently Asked About Rob Slade's Innumerable Book Reviews --

Now With Answers!

Questions and answers

1) How do you find time to read all those books?

Darned if I know. I've always read a lot, and quickly. No, I don't do speed

reading: I find that I can't use those techniques. I read while waiting, I

read while traveling: sometimes I just read. I read and review as much as I

can spare time for. Those who have followed the series of

reviews will notice that sometimes I produce more than others: a lot depends on what else I have to do at the time. Yes, I do read all of the books: every page (although, I admit, sometimes not every word).

2) Do you have an archive of the reviews?

Yes, two, in fact. The "base" URLs are <http://victoria.tc.ca/techrev>, courtesy of the Victoria, BC, Canada TelecommunityNet (aka VTN), and <http://sun.soci.niu.edu/~rslade>, courtesy of Northern Illinois University (former home of the Computer Underground Digest and aka NIU). All the various pages and files are in those directories, so you can construct a full URL by simply appending the filename. Also, all files are mirrored at both sites. For example, a reference in one review, like "(cf. BKVR.RVW)," would mean that the filename (converted to lower case) could be appended to the base addresses, and you would find that both <http://victoria.tc.ca/techrev/bkvr.rvw> and <http://sun.soci.niu.edu/~rslade/bkvr.rvw> point to actual reviews. (If you use only the base URLs, you will find an index file that points you at some of the major pages.)

For those looking for the reviews, probably the most useful addresses will be <http://victoria.tc.ca/techrev/mnbk.htm> or <http://sun.soci.niu.edu/~rslade/mnbk.htm>; the top level of the topical menus of book reviews (security is not the only topic); and <http://victoria.tc.ca/techrev/review.htm> or <http://sun.soci.niu.edu/~rslade/review.htm>; the main index to all reviews. Due to increasing numbers of questions, I guess I will

be
maintaining this FAQ at <http://victoria.tc.ca/techrev/revfaq.htm>
and
<http://sun.soci.niu.edu/~rslade/revfaq.htm>.

3) Where can I find the reviews?

All kinds of places, apparently. There are, of course, the archives above, and the various topically related lists and groups to which I post messages. Others archive various subsets of the reviews to different sites, reprint the reviews in college or user group newsletters, and repost the reviews to other mailing lists. If you want to get on a mailing list for all the reviews, I have created a mailing list at Yahoo Groups. You can subscribe by sending an email message to techbooks-subscribe@yahoogroups.com, or visiting the Web site at <http://groups.yahoo.com/list/techbooks/>, where you can also find an archive of the more recent reviews.

4) Don't you like *any* books?

OK, I'm a cruel reviewer. But fair!

But, yes, I do like some. In the absence of a "Rob's Picks" page (which I may get around to some time) the closest alternative is probably the page of references by the CISSP domains, at <http://victoria.tc.ca/techrev/mnbksccd.htm> or <http://sun.soci.niu.edu/~rslade/mnbksccd.htm>.

5) Why don't you rate the books you review?

Generally, the people who ask this question want me to assign a single numeric value, preferably on a scale of 1-5, to every book.

Books are a little bit more complex than that. They are good or bad for different reasons for different groups. A book for a novice is useless to an expert. A book for an expert is useless to a novice. So I try to state who I would recommend the book to, and why. I think it's a bit more reasonable than just giving each book a number.

If I'd wanted to do that, I could have skipped writing the reviews entirely. It'd sure save time. (See question 1 :-)

However, a partial answer, for those who want a quick fix, is to look at the main review index. (See question 2 :-) I try to give a summary of my reaction to the book, in not more than one sentence.

6) Where can I find your reviews of all the CISSP guides?

See <http://victoria.tc.ca/techrev/mnbkscci.htm> or <http://sun.soci.niu.edu/~rslade/mnbkscci.htm>.

7) What's all that stuff at the beginning?

I was asked by the moderators of one newsgroup to use the standard UNIX addlib format for publication information. It seemed to be a good set of data, so I continued. The basic information is:

```
%A Author's name (use a separate %A line for each)
%C City (place of publication)
%D Date of publication
%E Editor (of book or series)
%G Government order number (use this for ISBN)
%I Issuer (publisher's name and imprint)
%O Comments/etc. (use for format/price, ordering info)
    (also the links for purchase at online bookstores. Yes, I
do
    get a commission: see question 8.)
```

%P Page number(s) (use for page count)
%T Title of article or book

For more information, see the man page for the UNIX "refer" command.

8) How much money can you make reviewing books?

I find it quite bizarre that almost everyone seems to assume that a) I buy all these books, or b) I get paid for doing these reviews. I get the books free from publishers. (See question 9.) I don't get paid for doing the reviews. Occasionally I use these reviews as the basis for review columns or "best of" articles for magazines, and get a few bucks. If people "click-through" the links on the reviews and buy books, I get a commission. (Eventually my account may build up to enough money that they'll actually send me a cheque.) I even get a bit of a tax break by getting a "gift in kind" tax receipt when all these dead trees go to the library. But this isn't exactly a business.

Of course, if any large corporation was interested in sponsoring the reviews ... :-)

9) How can I get started reviewing books?

In the immortal words of the advertising campaign, just do it. Grab some books, and review them. Post the reviews. Once you have built a body of work, you can start asking publishers for copies of books, especially if you have proven you are serious by sending them copies of the drafts of your reviews. (Before you post them on the net.)

You don't even have to buy a ton of books to get started. Review

the ones
you've already got. If you use them, presumably you know why. If
you want to
review new ones, try the library. (If you live in Vancouver, the
Vancouver
Public Library has lots of recent technical books :-)

Of course, why would you want to? (See question 8.)

10) Where can I find books on (topic)?

Go to the main review index at <http://victoria.tc.ca/techrev/review.htm> or
<http://sun.soci.niu.edu/~rslade/review.htm>. Use the search
function on your
browser (Ctrl-F for most Windows stuff, "/" for Lynx, etc).
Search for terms
you think would be in the title or the topic of the book. (For
privacy you
might want to search on "privacy," "private," or
"confidential.") When you
find a likely title, there will be a link to the review itself.

=====

rslade@sprint.ca rslade@vcn.bc.ca slade@victoria.tc.ca
pl@canada.com

===== for back issues:

[Victoria Freenet] site <http://victoria.tc.ca/int-grps/books/techrev/>

or <http://www.victoria.tc.ca/techrev>

or <http://victoria.tc.ca/techrev>

an alternate site has been provided by CuD and NIU
at:

<http://sun.soci.niu.edu/~rslade/>

CISSP refs: [Victoria Freenet]mnbksccd.htm

PC Security: [Victoria Freenet]mnvrrrvsc.htm

Security Dict.: [Victoria Freenet]secgloss.htm

Security Educ.: [Victoria Freenet]comsecded.htm

Book reviews: [Victoria Freenet]mnbk.htm

[Victoria Freenet]review.htm

Partial/recent: <http://groups.yahoo.com/group/techbooks/>

Security Educ.: <http://groups.yahoo.com/group/comsecded/>

Review mailing list: send mail to techbooks-subscribe@egroups.com

★REVIEW: "Honeypots: Tracking Hackers", Lance Spitzner

Rob Slade <rslade@sprint.ca>

Mon, 10 Feb 2003 08:04:30 -0800

BKHNYPOT.RVW 20030126

"Honeypots: Tracking Hackers", Lance Spitzner, 2003, 0-321-10895-7,

U\$44.99/C\$69.99

%A Lance Spitzner hostmaster@tracking-hackers.com

%C P.O. Box 520, 26 Prince Andrew Place, Don Mills, Ontario
M3C 2T8

%D 2003

%G 0-321-10895-7

%I Addison-Wesley Publishing Co.

%O U\$44.99/C\$69.99 800-822-6339 fax 617-944-7273 bkexpress@aw.com

%O <http://www.amazon.com/exec/obidos/ASIN/0321108957/robsladesinterne>

%P 452 p. + CD-ROM

%T "Honeypots: Tracking Hackers"

Chapter one is an introduction to the honeypot concepts, and the story of

Spitzner's first attempt to run one. An overview of attackers and tools is

given in chapter two. A history of honeypots is provided in chapter three,

and a list of basic types. Chapter four looks at the benefits (and also the

problems) of these types of programs. The types of honeypots are grouped

into high, medium, and low interactivity, in chapter five. The explanations

given, in this first section, are good and simple. Tables and

figures
provided, however, often require interpretation.

Chapters six to eleven are reviews and descriptions of honeypots and related programs. There is a tutorial on the setup and use of Back Officer Friendly in chapter six. Specter, in chapter seven, gets a detailed review and a discussion of the program's options. Chapter eight discusses how honeyd emulates a network. Port monitoring, with netcat, and jails, using chroot, are covered in chapter nine. Mantrap cages are discussed in chapter ten. Chapter eleven reviews two generations of honeynets, with lots of details.

Chapter twelve examines choosing and camouflaging honeypots. Maintaining and using a honeypot is in chapter thirteen. Chapter fourteen presents a couple of "case studies," integrating material from previous chapters. There is a reasonable discussion of legal issues in chapter fifteen. Future directions for honeypots are examined in chapter sixteen.

"Know Your Enemy" (cf BKKNYREN.RVW) presented a fascinating glimpse into both honeypots and the blackhat community, but only a glimpse. This book provides much more detail into the inner workings, setup, and technologies involved in sensors for detecting and dissecting network intrusions.

copyright, Robert M. Slade, 2003 BKHNYPOT.RVW 20030126
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

<http://victoria.tc.ca/techrev/~rslade> or <http://sun.soci.niu.edu/~rslade>



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 57

Weds 19 February 2003

Contents

- [Playing Russian Roulette with traffic lights](#)
[Dan Foster](#)
 - [Scuba diving computer recall](#)
[Tom Race](#)
 - [Gambling on systems accountability](#)
[Irena Szrek](#)
 - [University software development fiasco](#)
[Identity withheld by request](#)
 - [Re: Identity theft evidently based on spoofing AOL](#)
[Identity withheld](#)
 - [REVIEW: "Mike Meyers' Certification Passport CISSP", Shon Harris](#)
[Rob Slade](#)
 - [REVIEW: "CISSP Training Guide", Roberta Bragg](#)
[Rob Slade](#)
 - [REVIEW: "Advanced CISSP Prep Guide: Exam Q & A", Krutz/Vines](#)
[Rob Slade](#)
 - [REVIEW: "The CISSP Prep Guide Gold Edition", Krutz/Vines](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ Playing Russian Roulette with traffic lights

Dan Foster <dsf@globalcrossing.net>

Wed, 19 Feb 2003 22:22:53 +0000

I came across a post by someone I know from previous posts in a travel USENET newsgroup -- Bill Mattocks, who mentioned an interesting cause of a car accident he was in on 2 Feb 2003 at the College and Nall intersection in Overland Park, Kansas.

He was driving towards an intersection that was apparently in a flashing four-way red traffic signal so all cars came to a full stop and yielded appropriately. He then proceeded to drive through the intersection when it was his turn and after having verified the intersection and immediate vicinity was clear of any potential hazards, and had the monumental bad luck of having entered the intersection just as the lights suddenly started working again and it had signalled green in the lane at a 90 degree angle to him.

End result? A BMW sped through the intersection, having seen a green, and didn't see his car until it was too late. (Both parties seems to be ok, with some minor injuries, fortunately.)

The RISKS? The light **didn't** fail safely. Well, it did fail safely by reverting to a four way flashing red light which is equivalent to a four way stop sign. However, if it was properly designed, it would not

have changed
into any other mode without manual intervention by someone
present at the
control box by the intersection, along with a police officer to
temporarily
handle the traffic at moment the lights were put back into
working order,
manually.

I realize that such an approach would have been burdensome in
certain
situations such as a large scale recovery after a power outage,
but it's
much less of a Russian Roulette-type of situation for drivers
("Is the light
going to suddenly indicate green or red in my direction if it
decides to
start working again?") when properly handled.

The crux being that there is no safe way to deterministically
recover from
such a failure without onsite manual intervention.

Perhaps something that the Department of Transportation (DOT)
and engineers
at Crouse-Hinds (a major traffic light manufacturer) might take
into
account?

Scuba diving computer recall

Tom Race <tom.race@skipton.co.uk>
17 Feb 2003 05:35:20 -0800

[See also Risks in scuba equipment, Carl Page, [RISKS-21.41](#)]

In simple terms, a dive computer monitors the amount of nitrogen
dissolved

in the diver's blood. Typically worn like a wrist watch, it tracks the diver's depth and calculates the absorbed nitrogen according to a mathematical model of the human body's various tissues.

If a diver surfaces too quickly with too much nitrogen in the body it is released as bubbles within the blood or tissues, potentially causing injury or death through Decompression Sickness (DCS). Divers typically rely heavily on a computer to tell them when to surface to avoid DCS.

The manufacturer below is being sued over the mathematical model, which has a faulty assumption, or more likely a complete oversight. The model embedded in this computer assumes that the diver on the surface continues to breath whatever gas mixture they were diving with. When the diver is using nitrox, a gas mixture containing extra oxygen and therefore less nitrogen than air, the computer will assume that they are releasing nitrogen at a higher rate than reality. Over several dives and several intervals on the surface, the state of the mathematical model and the diver's actual nitrogen levels may become seriously different, and in the 'wrong' (more risky) direction.

A failure of requirements specification or code inspection? The lawsuit refers to a 'manufacturing defect'.

I have an interest, since I have a nitrox computer from the same manufacturer. Fortunately mine is more recent, and I have not used it for gases other than air.

Tom Race

- - - - -
Uwatec, Scuba Pro and Johnson Outdoors Subject of Class Action
Seeking
Product Recall; 5 Feb 2003

Dive industry leaders Uwatec and Scuba Pro, and their parent company, outdoor equipment conglomerate Johnson Outdoors, Inc., have been sued in federal court by a former authorized reseller, Robert Raimo, seeking a mandatory recall of all Aladin Air X Nitrox dive computers manufactured before 1 Feb 1996. The suit seeks certification as a class action on behalf of all owners of the dive computers, and all persons who acted as retailers, dealers, wholesalers or distributors of the dive computers.

The suit claims that 1995 model Aladin Air X Nitrox dive computers have a manufacturing defect that prevents the computer from switching from underwater to surface, or air mode when the user returns to the surface. As a result, the computer continues to calculate a diver's decompression obligations as if the diver were breathing enriched air, or nitrox, containing as little as 50% nitrogen, while on the surface, instead of properly calculating the diver's decompression obligations and off-gassing while the diver is breathing air, which contains 78% nitrogen. This defect causes the computer to underestimate residual nitrogen loads, and to overestimate the diver's safe repetitive bottom times, thereby significantly increasing the diver's risk of contracting decompression sickness (bends).

The suit alleges that the defect is likely to affect experienced divers making multiple nitrox dives in a single day to maximize bottom time, such as those conducted on increasingly popular "live-aboard" dive vacations in exotic locations, far away from the nearest treatment centers capable of saving the life of a diver stricken with decompression sickness.

The so-called "air-switching defect" was first described in an internal Uwatec memo dated 30 Jan 1996, which warned one of the company's test divers about "the faulty Aladin Nitrox". The memo described how to manually override the defect so the diver could safely use his computer until it was replaced by Uwatec. After this memo was sent to Uwatec's U.S. management, they drafted a product recall notice. However, the suit alleges the managers were fired before they could issue the recall notice, and the defendants have maintained a "conspiracy of silence" ever since.

Copies of the 1996 memo and recall notice are attached as exhibits to the complaint and may be viewed on the News section of the Web site of Raimo's attorney, David Concannon, at www.davidconcannon.com.

Raimo was stricken with Type II decompression sickness after using a 1995 model Aladin Air X Nitrox on four nitrox dives off Bonaire in Apr 2002. He is the former owner of two retail dive centers in New York.

According to Concannon, the suit was filed as a class action only after Johnson, Scuba Pro and Uwatec rebuffed Raimo's requests that the companies

issue a voluntary recall. The suit was filed in Oakland, California because four other lawsuits filed by divers alleging they were injured by the same model computer are currently pending there and are scheduled for trial in Nov 2003.

Contact: David Concannon, 610-293-8084

David G. Concannon, Law Offices of David G. Concannon, LLC
Strafford Building One, Suite 112, 150 Strafford Avenue
Wayne, Pennsylvania 19087
Phone: (610) 293-8084 Fax: (610) 293-8086 concannonlaw@msn.com

✶ Gambling on systems accountability

Irena Szrek <irena_szrek@yahoo.com>

Sun, 16 Feb 2003 19:09:46 -0500

I read with interest Peter Neumann's article on 'Gambling on Systems Accountability' in the 'Inside Risks' section of the February 2003 *Communications of the ACM* (Volume 46, Number 2). I can not agree more with Peter's observations on current drawback of computer systems security and need to focus on system integrity rather than confidentiality. I feel that as long as systems will not be designed with security and integrity as part of the system, and will not provide effective and conclusive audit capabilities, they will be exposed to insider or outsider fraud and will be targets of (at times successful) attacks. This is especially true in industries where ability to gain large sums of money is at

stake, as in the off-track-betting systems Peter mentions, or in lottery and casino systems.

I want to mention an approach to stop insider fraud in gaming systems that use random numbers. Random-number generators are used in gaming to decide outcomes of games, and are used in electronic drawing machines to pick draw numbers. Typically, the only security present is physical security; the audit trail, if any, is of the generation process, which can be circumvented by a skilled insider. We have introduced a new notion of 'unpredictable auditable random numbers', where audit of outcomes is an element of system design. With the use of digital signature, random numbers can be generated in a way providing conclusive audit of the numbers themselves. This guarantees that a proper set of random numbers is used for the plays or the draws, and is not tampered with by dishonest insiders.

Irena Szrek, Szrek2Solutions 1-401-398-0395 <http://www.szrek.com>
irena@szrek.com <mailto:walter@szrek.com>

⚡ University software development fiasco

<[Identity withheld by request]>
Wed, 19 Feb 2003

If you are interested in yet another case of a large software project gone horribly wrong, then this is a beauty:

Back in the planning stages, we had a Director of IT who loathed UNIX. So he decreed that the new academic record system would run on Windows back-end systems. Oracle and Peoplesoft said, "You want to do what!?"

The new system was switched on in early November 2001 and the old system was simultaneously switched off. (NOTE, since we are in the Southern hemisphere, November is the time of peak demand for student grade processing, registration, etc.)

It is now over a year after the system was switched on. The system still does not provide several of the key features that were touted as the reasons for its implementation.

Information that has become public in the past year includes the fact that several U.S. universities have had significant problems with the system. And *their* version was simpler than ours since our university combines both a normal U.S. style university and an additional school that is a sort of combination VocationalTech and junior college. So, if it didn't work in the simpler U.S. environment, how could it possibly work here?

The problems and risks that are highlighted here include:

- 1) Choose the best platform for the job.
- 2) The "big-bang" approach to implementation is always a disaster waiting to happen. Frequently the disaster doesn't wait. There were three problems which compounded the problem. There had been no real stress testing of the new system, it was rolled-out at the time of peak demand,

and the old
system, which would otherwise have provided a backout option,
was
switched off.

3) Non-technical people driving technical decisions.

4) Overly complex and ambitious systems being implemented as a
single system
and all at once rather than being phased in.

Obviously, I'm sort-of on the inside on this, so I'd rather this
didn't get
published with my name. But, it is cautionary, at least to the
extent that
so many of the above problems keep getting repeated, in one form
or another,
year after year. I've been reading comp.risks for a long time
now and it
seems like some lessons are never learned.

✶ Re: Identity theft evidently based on spoofing AOL ([RISKS-22.56](#))

<[Identity withheld by request; same contributor as above]>

Wed, 19 Feb 2003

About a year ago, we had a student who created a page based on
the Hotmail
password change page and then spammed Hotmail users with a
poorly written
e-mail, in fractured English, which instructed them to click on
the link and
change their Hotmail password. We estimate that it was active
for no more
than an hour. At the time he was shut down he had more than 120
username/
password combinations.

Given the dodgy nature of the message from "Hotmail" and the fact that the URL was clearly of the form ,,,.edu,,, it makes me wonder about the extent to which people seem to suspend critical judgment when they connect to the Net.

I suppose that I shouldn't be so surprised, given the number of hoax virus messages that seem to regularly get forwarded.

★ REVIEW: "Mike Meyers' Certification Passport CISSP", Shon Harris

Rob Slade <rslade@sprint.ca>
Mon, 13 Jan 2003 08:20:51 -0800

BKMMCISP.RVW 20021106

"Mike Meyers' Certification Passport CISSP", Shon Harris, 2002, 0-07-222578-5, U\$29.99/C\$44.95

%A Shon Harris shonharris@hotmail.com www.intenseschool.com

%C 300 Water Street, Whitby, Ontario L1N 9B6

%D 2002

%G 0-07-222578-5

%I McGraw-Hill Ryerson/Osborne

%O U\$29.99/C\$44.95 +1-800-565-5758 +1-905-430-5134 fax: 905-430-5020

%O <http://www.amazon.com/exec/obidos/ASIN/0072225785/robsladesinterne>

%P 422 p.

%T "Mike Meyers' Certification Passport CISSP"

There is a "Check-In" foreword, which seems to be about the series, and an introduction that provides a very terse overview of the CISSP

(Certified Information Systems Security Professional) exam.

The book consists of ten chapters, one for each of the CBK (Common Body of Knowledge) domains. "Security Management Practices" demonstrates that the book is perhaps a bit too thin: illustrations and other materials from Harris' "All-in-One" guide (cf. BKCISPA1.RVW) appear, but most of the tutorial material is vague and generic. (When covering "controls," a vital concept in this domain, the text provides an "exam tip" that controls should be visible enough to deter misdeeds, but not visible enough to be avoided, but completely neglects the second axis of the control matrix, which covers deterrence, detection, and so forth.) The review questions at the end of the chapter are better than some, but still quite simplistic. As well as being limited, the content is suspect in places: a "cognitive password" is very insecure, and why would a retina scanner blow air into your eye? The "Computers 101" part of "Security Architecture and Models" is all right, although very brief and with significant gaps, but the formal models are simplified to a problematic extent (and the explanation of lattice models is flatly wrong). The "Physical Security" chapter is probably adequate for study purposes. Even after all of the above, I was surprised at how poor the material in "Telecommunications and Networking Security" was. The TCP/IP content is definitely insufficient, and specific errors are made in a number of areas (such as the ability of PPTP [Point-to-Point Tunneling

Protocol] to encrypt data). "Cryptography" is limited to little more than the terms involved, and it is odd how much space is wasted on editorial comment. (The text could also use a bit more organization: a number of topics appear, in isolation, at a fair distance away from related items.) "Disaster Recovery and Business Continuity" is terse, but possibly sufficient for study purposes. The material in "Law, Investigation, and Ethics" is problematic: it appears to be somewhat dated and has some important gaps, such as corporate liability, interviewing, and the process of incident response. A great deal of the content in "Application Development" seems to have been parroted without any understanding: the iterative class of systems development models are not collected, the spiral model description is incorrectly described, the point of Java as a hybrid of compilation and interpretation seems to have been completely lost, and the malware text is rife with errors. "Operations Security" doesn't have as many mistakes, but it seems to be pretty much of an unorganized grab bag of topics.

Yes, I can see the need (or desire) for a short and quick reference to the CISSP CBK. However, if you are going to take on that task, you have to make every single word (and figure) count. This book doesn't. Since McGraw-Hill also published "CISSP All-in-One Certification Exam Guide" they should probably have heeded the old dictum that "if it ain't broke, don't fix it." As it is, this work is well back in the CISSP pack, along with

"Secured

Computing" (cf. BKSCDCMP.RVW) and "CISSP for Dummies" (cf. BKCISPDM.RVW).

copyright Robert M. Slade, 2002 BKMMCISP.RVW 20021106

✈ **REVIEW: "CISSP Training Guide", Roberta Bragg**

Rob Slade <rslade@sprint.ca>

Tue, 11 Feb 2003 08:10:53 -0800

BKCISPTG.RVW 20030127

"CISSP Training Guide", Roberta Bragg, 2003, 0-7897-2801-X,
U\$69.99/C\$108.99/UK#50.99

%A Roberta Bragg Roberta.Bragg@mcpmag.com

%C 201 W. 103rd Street, Indianapolis, IN 46290

%D 2003

%G 0-7897-2801-X

%I Macmillan Computer Publishing (MCP)

%O U\$69.99/C\$108.99/UK#50.99 800-858-7674 info@mcp.com

%O <http://www.amazon.com/exec/obidos/ASIN/078972801X/>

robsladesinterne

<http://www.amazon.co.uk/exec/obidos/ASIN/078972801X/>

robsladesinte-21

%O <http://www.amazon.ca/exec/obidos/ASIN/078972801X/>

robsladesinterne

%P 727 p. + CD-ROM

%T "CISSP Training Guide"

The introduction and frontmatter appear to be much more concerned with the structure of the book (and this particular series of books) than the CISSP (Certified Information Systems Security Professional) exam. The initial list of topics covered by the domains has notable gaps and some oddities in

organization.

Part one is entitled "Exam Preparation," and is divided into the ten standard domains of the CBK (Common Body of Knowledge). Chapter one, on access control, shows problems right away. The first paragraph tries to distinguish between access control and authentication, but doesn't really outline the relationship between the two concepts, let alone dealing with the broader and more usual interrelated ideas of identification, authentication, authorization, and accountability. When discussing access models, the lattice content touches on advanced outcomes of the model, but not the basic principles. The biometric material is simply inadequate. There are sample questions at the end of the chapter, and this first set, at least, do appear to be crafted in order to avoid the usual "reading check" level of simplicity, but the wording is extremely poor and many answers are either flatly wrong or highly misleading. Similar problems are evident with telecommunications and networking, in chapter two, which has excessive space given to topics like cabling characteristics, poor explanation of the relationship between tunnelling and virtual private networks, an overview of intrusion detection that contradicts the material in chapter one, and some completely idiosyncratic terminology. The answers to sample question are more correct, but only because the questions themselves are overly simplistic. The rudimentary factors of security management are discussed in chapter three, but in a confused fashion, not assisted by the fact that

topics are repeated and sections from other domains are introduced for no apparent reason. The central material is very brief, despite the sixty pages devoted to the topic, and entire sections, such as the various evaluation criteria, are missing. Applications development, in chapter four, does possibly provide enough information to deal with the CISSP exam on this subject, but lists lots of problems without many solutions, and has a great deal of extraneous material such as lists of different types of memory (fast page mode [FPM] versus extended data out [EDO] dynamic random access memory, for example). I thought the introduction to cryptography, in chapter five, wasn't all that bad (absent details such as the key in a one time pad having to be no shorter than the message being sent). That is, until I realized that it was the entire chapter, and details about any form of encryption, digital signatures, and the requirements for certification and a public key infrastructure were completely missing. Chapter six does cover the elemental points of security architecture, but in a disorganized manner, and has no material at all dealing with computer architecture. Operations security is discussed in terms of details like specific logs in Windows 2000 and updating antiviral scanners, and chapter seven misses more general concepts and operating principles. Business continuity and disaster recovery planning, in chapter eight, does provide most necessary information about the process, except for the recovery phase. Law, in chapter nine, concentrates too heavily on US legislation, and the

investigative process fails to address incident response, interviewing, and relations with outside agencies. Chapter ten again covers physical security with specific details rather than underlying concepts.

Part two is a review. About half of the "Fast Facts" are useful and the rest aren't: it would be hard for an exam candidate to know which is which. The study and exam prep tips are generic, and probably not much help. The practice exam questions are, like most of the sample questions in the book, far too simplistic and particular to properly prepare candidates for the actual CISSP exam.

Despite the size of this volume, it does not contain as much information as, say, Harris' "CISSP All-in-One Certification Exam Guide" (cf. BKCISPA1.RVW), nor is it organized as well as the Krutz and Vines work (cf. BKCISPPG.RVW). It is closer to the Endorf (cf. BKSCDCMP.RVW), Miller/Gregory (cf. BKCISPDM.RVW), or the second Harris (cf. BKMMCISP.RVW) works, and therefore its utility as preparation for the CISSP exam is questionable.

copyright, Robert M. Slade, 2003 BKCISPTG.RVW 20030127
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

<http://victoria.tc.ca/techrev/~rslade> or <http://sun.soci.niu.edu/~rslade>

⚡ REVIEW: "Advanced CISSP Prep Guide: Exam Q & A", Krutz/Vines

Rob Slade <rslade@sprint.ca>

Wed, 5 Feb 2003 08:28:24 -0800

BKADCIPG.RVW 20030110

"Advanced CISSP Prep Guide: Exam Q & A", Ronald L. Krutz/Russell Dean

Vines, 2003, 0-471-23663-2, U\$50.00/C\$77.50/UK#37.50

%A Ronald L. Krutz

%A Russell Dean Vines

%C 5353 Dundas Street West, 4th Floor, Etobicoke, ON M9B 6H8

%D 2003

%G 0-471-23663-2

%I John Wiley & Sons, Inc.

%O U\$50.00/C\$77.50/UK#37.50 416-236-4433 fax: 416-236-4448

%O <http://www.amazon.com/exec/obidos/ASIN/0471236632/>

[robsladesinterne](#)

%P 331 p. + CD-ROM

%T "Advanced CISSP Prep Guide: Exam Q & A"

Like "The Total CISSP Exam Prep Book" (cf. BKTCIEPB.RVW) before it, this

volume contains no tutorial material, only questions, and then questions and

answers. The format is quite similar to the Peltier work, with the book

divided into the standard ten domains. A major difference is the inclusion

of a CD-ROM with a testing engine. Every CISSP candidate wants sample exams

and sample questions, so the query remains, are the questions any good?

The CD-ROM contains "the Boson-powered test engine," but the questions are

not quite as simplistic as those on the Boson exams. They tend to be

longer, and, at first glance, look a lot more like real CISSP exam

questions. However, upon closer examination, two problems become obvious.

One is that a number of the questions are still very simple, despite the additional verbiage. They concentrate on pure recitation of facts, without the analysis and critical thinking that the actual exam requires. The second issue is that a large number of questions rely on very specific, and often esoteric facts. Again, this is counter to the genuine test, where concepts and principles are emphasized.

Occasionally these two difficulties combine in a single question, such as "Which choice below is NOT one of NIST's 33 IT security principles?" If you haven't fully memorized NIST's 33 security principles, don't worry. Even if you have no idea where to find NIST's 33 security principles you can still get the answer. One of your options is "Totally eliminate any level of risk." Even the rawest security neophyte can tell you that, since this is impossible, it obviously has to be the right answer.

This book may give you a somewhat better idea of the types of questions you may encounter, and the range of topics you may need to know. As preparation for the exam, however, it will both scare you unnecessarily (although if it drives you to take the ISC2 course, that might not be a bad thing), and fail to prepare you fully.

copyright Robert M. Slade, CISSP, 2003 BKADCIPG.RVW 20030110
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

<http://victoria.tc.ca/techrev/~rslade> or <http://sun.soci.niu.edu/>

REVIEW: "The CISSP Prep Guide Gold Edition", Krutz/Vines

Rob Slade <rslade@sprint.ca>

Wed, 12 Feb 2003 08:04:50 -0800

BKCIPGGE.RVW 20030130

"The CISSP Prep Guide Gold Edition", Ronald L. Krutz/Russell Dean Vines, 2003, 0=471-26802-X, U\$80.00/C\$124.50/UK#59.50

%A Ronald L. Krutz

%A Russell Dean Vines

%C 5353 Dundas Street West, 4th Floor, Etobicoke, ON M9B 6H8

%D 2003

%G 0=471-26802-X

%I John Wiley & Sons, Inc.

%O U\$80.00/C\$124.50/UK#59.50 416-236-4433 fax: 416-236-4448

%O <http://www.amazon.com/exec/obidos/ASIN/047126802X/>

[robsladesinterne](#)

<http://www.amazon.co.uk/exec/obidos/ASIN/047126802X/>

[robsladesinte-21](#)

%O <http://www.amazon.ca/exec/obidos/ASIN/047126802X/>

[robsladesin03-20](#)

%P 944 p. + CD-ROM

%T "The CISSP Prep Guide Gold Edition"

I happened to notice, in the preparation of this review, that a certain

online bookstore has a special in relation to this title. You can buy it,

along with the "Advanced CISSP Prep Guide: Exam Q & A" for a price slightly

less than that of the two volumes together. Pity those who take the

bookstore up on their offer: this volume is nothing more than "The CISSP

Prep Guide" (cf. BKCISPPG.RVW) and "Advanced CISSP Prep Guide: Exam Q & A"

(cf. BKADCIPG.RVW) bound together.

The authors have done some updating: there are, for example, a few additional pages of material on wireless security. The authors have improved their coverage of the Common Criteria--by reprinting the explanation that is provided on the National Institute of Standards and Technology (NIST) Web site.

Overall, however, the same comments appropriate to Krutz and Vines' original books still apply, so what I said was, for those studying for the CISSP exam, this book does provide a guide to the topics to be covered. If you are confident that you know more than the book at every point, you should be in good shape to sit the exam: if not, you will have to get help somewhere else. If you are studying for another security course, or are a security professional, this work will not have much to offer you. This volume may give you a somewhat better idea of the types of questions you may encounter, for the CISSP exam. As preparation for the exam, however, it will both scare you unnecessarily and fail to prepare you fully.

copyright, Robert M. Slade, 2003 BKCIPGGE.RVW 20030130
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

<http://victoria.tc.ca/techrev> or <http://sun.soci.niu.edu/~rslade>

✶ More-Than-Abridged info on RISKS (comp.risks)

<RISKS-request@csl.sri.com>

19 Feb 2003

[See www.risks.org for the archives of back issues, almost all of which include info on RISKS. (This issue is an exception.) PGN]



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

[ACM](#) Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 58

Friday 21 February 2003

Contents

- [Surgeons transplant mismatched organs](#)
[Steve Klein](#)
- [Health threat from computer use](#)
[Pete Mellor](#)
- [INFOSEC issues reach out to elevators](#)
[Russ Cage](#)
- [A \\$55,000 Net scam warning](#)
[Monty Solomon](#)
- [FTD.com hole leaks personal information](#)
[Fuzzy Gorilla](#)
- [ATM vulnerabilities and citibank's gag attempt](#)
[Ross Anderson](#)
- [Microsoft steamed over Hotmail spam](#)
[NewsScan](#)
- [Deadly input validation?](#)
[Chris Adams](#)
- [Fire risks](#)
[Tony Jones](#)
- ["E-lip" telemarketing phone systems](#)
[Al Meers](#)

- [Web site product serial number validation](#)
[Nik Smith](#)
 - [Two-digit year field strikes again](#)
[Fuzzy Gorilla](#)
 - [Too much tech can kill you](#)
[Jesus Climent](#)
 - [Lawyers say hackers are getting bum rap](#)
[NewsScan](#)
 - [Re: Playing Russian Roulette with traffic lights](#)
[Nicholas Weaver](#)
 - [The fourth solution...](#)
[Peter da Silva](#)
 - [REVIEW: "Mike Meyers' Security+ Certification Passport", Trevor Kay](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✂ Surgeons transplant mismatched organs

Steve Klein <steveklein@mac.com>

Thu, 20 Feb 2003 11:44:33 -0500

On 7 Feb 2003, doctors at Duke Hospital in North Carolina mistakenly transplanted a heart and lungs from a donor with Type A blood to a recipient with Type O blood. Her body immediately started rejecting the transplanted organs. The organs, which came from a cadaver in Massachusetts, included paperwork correctly listing the donor's type-A blood. The hospital admits the error, but hasn't made public any information indicating how the mistake was made.

On 20 Feb, new matching organs were transplanted in a second surgery. Under

normal conditions, a heart-lung transplant has a 50% success rate.

[I have yet to hear whether there was any computer-related error here --

for example, someone miskeying the patient's blood type as A or misrepresenting the donor's type as O. Please let us know if you hear anything further. PGN]

⚡ Health threat from computer use

Pete Mellor <pm@csr.city.ac.uk>

Mon, 10 Feb 2003 01:09:44 +0000 (GMT)

Sitting too long at your computer can cause potentially deadly blood clots.

The European Respiratory Journal reports the case of a young man from New

Zealand who nearly died after developing deep-vein thrombosis (DVT) after

using his computer as much as 18 hours a day. The clot in his leg broke off

and traveled to his lungs. (This problem has been reported on long airline

flights, and was reportedly first noticed in people who sat in World-War-2

air-raid shelters). [Source: BBC news, 28 Jan 2003; PGN-ed]

<http://news.bbc.co.uk/1/hi/health/2698119.stm>

Peter Mellor, Centre for Software Reliability, City University, Northampton

Square, London EC1V 0HB +44 (0)20 7040 8422

⚡ INFOSEC issues reach out to elevators

Russ Cage <russcage937362@yahoo.com>

Thu, 20 Feb 2003 17:22:37 -0800 (PST)

The RISKS of the following should be obvious to regular readers of this forum. Emphasis IN CAPITALS added by poster, not in original.

INTERNET LIFT CONTROL: Alcala University's Electronic Department has a research group that is developing an electronic system that will monitor the operation state of an elevator and transmit that information through the Internet to a central computer. The system would be installed in each lift with temperature-gauge inputs in various locations. The transmission signals WILL PERMIT THE MACHINERY TO BE RESET AND ACTED UPON BY REMOTE CONTROL. Collaboration is being sought through a joint venture or a licensing/manufacturing agreement. ELENET(R) is a free e-mail newsletter transmitted biweekly by Elevator World, Inc., the publisher of ELEVATOR WORLD magazine. ELENET(R) is a registered trademark and all rights are reserved. Copyright 2003(C) Elevator World, Inc., 356 Morgan Avenue, Mobile, AL 36606, phone: (251) 479-4514, fax: (251) 479-7043, Internet: www.elevator-world.com.

[I got a real UPLIFT from reading that one. I hope it PUSHES YOUR BUTTONS as well. In elevator parlance, it could RUS(S)tle your CAGE. I note that the Spanish word for elevator is "ascensor", which suggests that we might contemplate the SENSOR CENSOR that filters the

information

that is available to the Internet when a Critical Person or someone with

a large rear end (as*censor) enters the elevator, and perhaps even a

SEE-YOU-LATER-ALLOCATOR ACTUATOR when you wish to delay someone you

don't like. PGN]

⚡ A \$55,000 Net scam warning

Monty Solomon <monty@roscom.com>

Tue, 28 Jan 2003 00:22:29 -0500

Despite being described as a long-time Internet user and an accomplished

dentist who was knowledgeable about Internet crime, Bruce Lachot decided to

buy a new BMW M5 over the Internet from someone in Germany, for the bargain

price of \$55,000. The result: no car, no trace of the seller, and the need

for a lot more dental patients. [Bob Sullivan, MSNBC, 23 Jan 2003; PGN-ed]

<http://www.msnbc.com/news/854552.asp>

⚡ FTD.com hole leaks personal information

"Fuzzy Gorilla" <fuzzygorilla@euroseek.com>

Sat, 15 Feb 2003 15:55:52 -0500

A security flaw at FTD.com left a large flowering bouquet of private

information ready for picking during the busy business week

leading up to Valentine's Day. Using sequentially modified cookies, outsiders could exhaustively access customer billing records, including names, addresses, and phone numbers. (Availability of credit-card data was reported initially, but later denied by FTD -- perhaps after they blocked it.) This was discovered when one customer found another person's information displayed by his browser, and reported to NTBugTraq on 12 Feb. It was fixed on 14 Feb. Prerequisite for doing the attack was reported as 'HTML for Dummies' (or equivalent).

[Source: Robert Lemos, FTD.com hole leaks personal information, CNET News.com, 13 Feb 2003; PGN-ed]

<http://news.com.com/2100-1017-984585.html>

✶ ATM vulnerabilities and citibank's gag attempt

Ross Anderson <Ross.Anderson@cl.cam.ac.uk>

Thu, 20 Feb 2003 09:58:47 +0000

[See the cryptome.org URL below, which is one of the sites at which

this message and its supporting documents appeared. PGN]

Citibank is trying to get an order in the High Court today gagging

public disclosure of crypto vulnerabilities:

http://www.cl.cam.ac.uk/ftp/users/rja14/citibank_gag.pdf

I have written to the judge opposing the order:

http://www.cl.cam.ac.uk/ftp/users/rja14/citibank_response.pdf

The background is that my student Mike Bond has discovered some really horrendous vulnerabilities in the cryptographic equipment commonly used to protect the PINs used to identify customers to cash machines:

<http://www.cl.cam.ac.uk/TechReports/UCAM-CL-TR-560.pdf>

These vulnerabilities mean that bank insiders can almost trivially find out the PINs of any or all customers. The discoveries happened while Mike and I were working as expert witnesses on a 'phantom withdrawal' case.

The vulnerabilities are also scientifically interesting:

<http://cryptome.org/pacc.htm>

For the last couple of years or so there has been a rising tide of phantoms. I get e-mail with increasing frequency from people all over the world whose banks have debited them for ATM withdrawals that they deny making. Banks in many countries simply claim that their systems are secure and so the customers must be responsible. It now looks like some of these vulnerabilities have also been discovered by the bad guys. Our courts and regulators should make the banks fix their systems, rather than just lying about security and dumping the costs on the customers.

Curiously enough, Citi was also the bank in the case that set US law on phantom withdrawals from ATMs (Judd v Citibank). They lost. I hope that's an omen, if not a precedent ...

⚡ Microsoft steamed over Hotmail spam

"NewsScan" <newsscan@newsscan.com>

Wed, 19 Feb 2003 08:38:14 -0700

Microsoft has filed a lawsuit against unnamed bulk mailers who harvested the e-mail addresses of Hotmail users in order to bombard them with junk messages. The spammers allegedly used tools to randomly generate e-mail addresses and then tested them to see which accounts were active. Microsoft argues that this form of dictionary attack violates federal laws, including the Computer Fraud and Abuse Act. (*The Register*, 19 Feb 2003; NewsScan Daily, 19 Feb 2003)

<http://www.theregister.co.uk/content/6/29382.html>

⚡ Deadly input validation?

Chris Adams <chris@improbable.org>

Tue, 18 Feb 2003 22:00:39 -0800

Two teenagers died when their rowboat sank in Long Island Sound on 24 Jan 2003. The 911 operators who took their last-minute phone call have been charged for not handling the call and delaying the search for a day. The story suggests that there may have been some familiar RISKS themes along with the obvious ones: the operator attempted to enter "Long Island Sound"

as the location but the software prevented that and, after consulting an equally ill-informed supervisor, the operator simply gave up and dropped the call. It sounds like this was a known problem as the official response has been that they should have known to use the address of the nearest police station instead. http://story.news.yahoo.com/news?tmpl=story&ncid=533&e=9&cid=533&u=/ap/20030218/ap_on_re_us/missing_teens

Fire risks

Tony Jones <tmj@apex.net.au>
Fri, 21 Feb 2003 07:13:57 +1100

A newly-available Web site at <<http://www.sentinel.csiro.au/>> declares:

"Sentinel Fire Mapping is a mapping tool designed to provide timely fire location data to emergency service managers across Australia. The mapping system allows users to identify fire locations that pose a potential risk to communities and property."

Unfortunately, recent publicity for the site has generated a burning interest:

"Due to heavy demand this Web site is currently experiencing delays. Please be patient and allow priority access to emergency services."

✶ "E-lip" telemarketing phone systems

<AlMeers@aol.com>

Fri, 21 Feb 2003 10:44:39 EST

I got a fundraising phone call last week from one of the US political party's campaign fund raising organizations. This alerted me to a new type of phone-calling mechanism that more and more telemarketers are using. While the voice on the other end of the line was human, there were odd pauses between portions of our conversation, a few clicks on the other end of the phone line, and sometimes an odd response to my questions or comments.

I realized that I was talking to a machine which was being controlled by a human. Not an "Eliza" like computer program mind you, but a recorded voice mechanism which a human was controlling. Half of the responses were totally appropriate, accurate, and well-delivered, but the rest seemed that "he" was not really listening to me, or had to read from a pre-canned and scripted set of responses.

Well, of course that is exactly what was going on. The human telemarketer would be listening to the call, and in response to my questions, comments, and responses, push a button on a computer screen which would then play a prerecorded statement in answer to my query. It was fairly easy to ask a couple of offbeat questions which could only be handled by vague, stiff, and

rather useless zombie-like answers.

The system can actually be quite useful in many circumstances where the phone operators repeat the exact same answers many times during the day. A live operator can sound bored, angry, distracted, or have a hard time to understand accent, where the prerecorded voice is always pleasant, clear, and can even have the same regional or national accent of the caller.

These same human controlled computer response "e-lip" systems are not just useful in telemarketing, they can also be useful in phone Customer support environments, at least on the front line calls.

And in an Internet "chat" room support environment, one technician could carry on multiple conversations simultaneously, responding by copy&pasting pre-canned text to a screen full of slow typists. In a chat-room environment, the delay in responses would barely be noticed unless the tech was trying to do too many conversations at once.

<http://sfgate.com/cgi-bin/article.cgi?f=3D/c/a/2003/02/19/LAZ.TMP> details a SBS Yahoo tech call with "Floyd" and support.sbcglobal.net/general/contact/ can connect you with "Austin".

Both are apparently a form of "e-lip" systems.

The risk here is that inappropriate responses from a "known" machine can be tolerated to some extent, but my tolerance level shrunk to almost zero when I realized that I was being "fooled" into thinking I was actually talking with a human. There is a difference between talking WITH a

person, and talking AT a person who is responding via a canned-response machine. If I was talking to Stephen Hawking, the machine responses are "normal", but these systems are attempting to fake you out, and those same responses evoked frustration, resentment, and maybe even anger.

After playing with the "cyborg machinery" for a few seconds I just hung up.

✶ Web site product serial number validation

"Nik Smith" <nik@djnz.com>
Thu, 20 Feb 2003 18:01:41 -0000

Ok, I know it's not much of a security issue, but to leave the code in your Web page viewable to see what format the 'valid serial number' should be is just silly.

I wanted to download a patch for my lecturer to run a copy of 3dstudio

max on XP, and went to www.discreet.com to do this:

(Yes, they have licenses, but the software version they use won't work on XP)

www.discreet.com/support/max

where I was prompted for my name, surname, address, serial number of the product etc in order to obtain the update.

After being told I had entered incorrect details persistently, I thought

I'd check the source code to see what it wanted. Yep, there it was:

```
function ValidSerial(item) {
  if (item.length != 12) return false;
  if (item.indexOf('-') != 3) return false;
  var i;
  for (i = 0; i < item.length; i++) {
    var c = item.charAt(i);
    if (((c < "0") || (c > "9")) && (i != 3)) return false;
  }
  if (item == "226-19791979") return false;
  if (item == "110-12345678") return false;
  return true;
}
```

So, in goes a random number in the format clearly described, and away I go.

A valid street name and postal code can be obtained from www.streetmap.co.uk

and typing in a random street name, and an e-mail address, should they need

to send you an activation code or such like, can be set up at hotmail

instantly. The least they could've done is use .asp to hide the code. One

easy way to avoid disclosing your personal information to companies you'd

rather not have it.

Nik, student at BCUC(.ac.uk)

Two-digit year field strikes again

"Fuzzy Gorilla" <fuzzygorilla@euroseek.com>

Fri, 31 Jan 2003 18:22:21 -0500

In Norway, a 106-year-old woman was summoned to start school, and offered

free bus rides to the school. The last time she had started school was of

course 1903, having been born in '97. "Since I can already

read, maybe I should skip a couple grades," she joked. [Source: Associated Press, 31 Jan 2003; PGN-ed]

<http://news.yahoo.com/news>

[?tmpl=story2&u=/ap/20030131/ap_on_fe_st/norway_senior_student](http://news.yahoo.com/news?tmpl=story2&u=/ap/20030131/ap_on_fe_st/norway_senior_student)

⚡ Too much tech can kill you

Jesus Climent <jesus.climent@hispalinux.es>

Thu, 20 Feb 2003 12:33:12 +0100

As a proof that technology can lead to a dead end, here it goes what happened last winter to my girlfriend and me. While visiting Portugal, in Lisbon, we had to go to the doctor. The medical insurance she is subscribed to allows her to receive medical assistance without any bills, which are sent to the insurance company. For the only purpose of being sure that the carrier of the insurance title the insurance company is asked to send a fax copy of the actual contract.

Oh well. That is not as easy as it sounds. When called, the company representative who answered the 24hrs service line said "we don't do faxes anymore. Don't they have an e-mail address?" It happens that in the 24 service hospital we went to, they do not have e-mail. And for that matter, what kind of authentication mechanism both ends would have used to ensure that the sender was who it claimed to be?

As seen, early technology adoption with a depreciation of old communication methods is as bad as slow technology adoption.

Finally we had to pay the bill. She will probably sue the company ;)

Jesus Climent | Unix SysAdm | Helsinki, Finland | pumuki.hispalinux.es

🔥 Lawyers say hackers are getting bum rap

"NewsScan" <newsscan@newsscan.com>

Fri, 21 Feb 2003 10:39:34 -0700

The National Association of Criminal Defense Lawyers has joined with the Electronic Frontier Foundation and the Sentencing Project in publishing a position paper that argues people convicted of computer-related crimes tend to receive harsher sentences than perpetrators of comparable non-computer-related offenses. "The serious nature of the offenses is overplayed," says Jennifer Granick, author of the paper and clinical director at Stanford University's Center for Internet and Society. "The (majority) of the offenses are generally disgruntled employees getting back at the employer or trying to make money." In a review of 55 cases prosecuted under the most-often used computer crime statute, only 15 involved harm to the public and only one resulted in a threat to safety. Those convicted "are receiving sentences based on the fear of the worst-case scenario rather than what the case may really be about," says Granick. The paper

was submitted in response a request for public comment by the U.S. Sentencing Commission as required by the Homeland Security Act of 2002. Cybercrime legal expert Scott Frewing says he agrees with many points raised in the paper, but recommends a two-tiered sentencing threshold: "I would be comfortable in a situation where the code addresses the discrepancy between those who cause bodily injury and those that don't. If that results in the law being unfair to a virus writer, maybe that's enough to put them on notice." [CNet News.com 20 Feb 2003; NewsScan Daily, 21 February 2003]

http://news.com.com/2100-1001-985407.html?tag=fd_top

✶ Re: Playing Russian Roulette with traffic lights (Foster, [R-22.57](#))

Nicholas Weaver <nweaver@CS.berkeley.edu>

Wed, 19 Feb 2003 17:25:58 -0800

[Dan Foster said "there is no safe way to deterministically recover" from the failure he described in [RISKS-22.57](#). PGN]

Actually, there is a reasonably "safe" automatic recovery procedure for traffic lights to transition from blinking-red to normal operation: Switch to red in all directions for the 10-20 seconds, in order to clear the intersection of those who were crossing in 4-way stop mode. This allows the intersection to clear of traffic before normal operation resumes.

You can pick nits on cases where a car ends up being stuck in the

intersection after the light resumes normal operation, but those can occur during normal operation as well.

[Congratulations to RISKS readers who responded to this one. We received over 100 messages, mostly with content similar to Nicholas's. Many thanks. That sets the all-time RISKS record thus far. CHEERS! PGN]

✶ The fourth solution... (Re: SQL Slammer, [RISKS-22.52](#))

Peter da Silva <peter@abnm.com>
28 Jan 2003 19:45:22 GMT

> As usual the two most common responses are:
> 1. Blame Microsoft for producing code with holes in.
> 2. Blame the sysadmins for not patching systems.
> [and 3. Nobody blames the anti-social [deleted] who wrote it]

My reaction is to blame the sysadmins who exposed a system to the Internet running unhardened applications without minimal firewalls in place. I have one Internet-visible box running SQL server... it's isolated behind a proxy firewall that doesn't allow any connections in or out that aren't specifically required for the application running on top of the database. This is really the appropriate level of protection for an application that's only "LAN tight"... regardless of who wrote the OS or application.

I wouldn't demand everyone use a proxy firewall, but I would expect at least as much protection between it and the Internet, and between the

inside LAN
and it, as there is between the inside LAN and the Internet.

But even the elementary precaution of restricting incoming connections to ports and addresses that are known to be required would have been enough to stop this worm in its tracks.

REVIEW: "Mike Meyers' Security+ Certification Passport", Trevor Kay

Rob Slade <rslade@sprint.ca>
Thu, 20 Feb 2003 07:48:41 -0800

BKMMSCR.P.RVW 20030207

"Mike Meyers' Security+ Certification Passport", Trevor Kay, 2003,

0-07-222741-9, U\$29.99/C\$44.95

%A Trevor Kay trevor@treverkay.com

%C 300 Water Street, Whitby, Ontario L1N 9B6

%D 2003

%G 0-07-222741-9

%I McGraw-Hill Ryerson/Osborne

%O U\$29.99/C\$44.95 800-565-5758 fax: 905-430-5020

%O <http://www.amazon.com/exec/obidos/ASIN/0072227419/>

[robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/0072227419/)

<http://www.amazon.co.uk/exec/obidos/ASIN/0072227419/>

[robsladesinte-21](http://www.amazon.co.uk/exec/obidos/ASIN/0072227419/)

%O <http://www.amazon.ca/exec/obidos/ASIN/0072227419/>

[robsladesin03-20](http://www.amazon.ca/exec/obidos/ASIN/0072227419/)

%P 363 + CD-ROM

%T "Mike Meyers' Security+ Certification Passport"

Given the organization of the Security+ objectives, part one covers general security concepts and chapter one is on access control. Some

factors are dismissed a little bit too concisely: it is difficult to justify the blanket statement that biometric authentication is "extremely accurate and secure."

(Biometrics does get a bit more explanation in the chapter on physical security, but there is no indication of that in this location.) For the first set of sample questions, the emphasis is on simple definitions and fact recitation, but later questions do become somewhat more complex. A variety of attacks are described in chapter two, generally reasonably. The virus material is unfortunately poor, concentrating on older viral technologies (such as the almost extinct boot sector viruses and older DOS precedence-based companions) and failing to provide proper outlines of the basic antivirus technologies.

Part two looks at communications security. Chapter three deals with remote access, but the content has limited application to security. Technologies related to Internet application security are reviewed in chapter four. The highlights are touched on, but the lack of detail can be troubling. Cookies are discussed, with some mention of privacy, but the potential problem of cross-site tracking is not dealt with at all, and neither is the danger of HTML (HyperText Markup Language) formatted messages when the topic turns to e-mail. The material on wireless networking and security, in chapter five, is very weak. The explanation of direct-sequence spread spectrum is not clear at all, a mention of SSL (Secure Sockets Layer) makes no reference to

the description in the previous chapter (and almost contradicts it), and security itself gets short shrift in the haste to trot out the alphabet soup of related technologies.

Part three deals with infrastructure security. Chapter six runs through a list of networking components, cabling, and storage media, again with limited allusion to security. Network topologies and intrusion detection systems are discussed in chapter seven. System hardening, generally by applying patches and disabling functions, is reviewed in chapter eight.

Cryptography is in part four. Most of the basic content in chapter nine is sensible, but it is clear from the paragraphs on double- and triple-DES (Data Encryption Standard) that the author does not fully understand the subject. Chapter ten reviews key management, but it is not clear why the topic was separated from that of PKI (Public Key Infrastructure).

Part five deals with operational and organizational security. Physical security, in chapter eleven, is covered fairly well. Disaster recovery is confined to backups and fault tolerance: chapter twelve supports Kenneth Myers contention (cf. BKMGTCPD.RVW) that most people concentrate on recovering technology rather than the business, and would be improved by a broader view that incorporated all aspects of the operation. Chapter thirteen lists some areas that should be covered in a security policy. Forensics is dealt with poorly, and chapter fourteen also throws in

education and training.

While the book still adheres, rather slavishly, to the arbitrary structure of the Security+ list of objectives, the content is generally pretty reasonable, providing background explanations for important concepts, and keeping the descriptions of many of the specific technologies limited to the fundamental ideas. The text does tend to be terse, given the size of the book, but most basic material should be available to the student. This does vary by chapter: some seem to be merely going through the motions. The work could be improved with some removal of duplicated material. For example, there are three separate discussions of social engineering, and two could be replaced with cross-references. Despite its smaller size, I would recommend this volume over the Syngress "Security+ Study Guide and DVD Training System" (cf. BKSCRTYP.RVW), but not emphatically.

copyright, Robert M. Slade, 2003 BKMMSCR.P.RVW 20030207
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

<http://victoria.tc.ca/techrev/~rslade> or <http://sun.soci.niu.edu/~rslade>



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 59

Weds 26 February 2003

Contents

- [Star Wars exempt from OVERSIGHT, REPORTING, AND TESTING requirements?](#)
[PGN](#)
- ["Bugsplat"--collateral damage simulator](#)
[Daniel P.B. Smith](#)
- [Scientology critic fined for undeclared file](#)
[Mark Thorson](#)
- [eBay: Big Brother is watching you, and documenting](#)
[Monty Solomon](#)
- [Telepathy used to defend voting systems?](#)
[Rebecca Mercuri](#)
- [Voting machine engineer sues, alleges machine design flaws](#)
[Susan Marie Weber](#)
- [Latest spam scam](#)
[Jim Griffith](#)
- [Nigerian slain over e-mail scam](#)
[John F. McMullen](#)
- [Spain - Vodafone sees its network crash after maintenance](#)
[Henry Baker](#)
- [An unexpected bill](#)
[Geoffrey Brent](#)

- [Re: Surgeons transplant mismatched organs](#)
[K P](#)
 - [Re: Deadly input validation?](#)
[Ed Ravin](#)
 - [REVIEW: "Building Secure Wireless Networks with 802.11", Khan/Khwaja](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

★ Star Wars exempt from OVERSIGHT, REPORTING, AND TESTING requirements?

"Peter G. Neumann" <neumann@csl.sri.com>
Mon, 24 Feb 2003 14:46:49 -0800 (PST)

Noted deep in the White House's proposed FY2004 budget, the administration is proposing to exempt the Pentagon's controversial national missile defense system from operational testing legally required of every new weapons system in order to deploy it by 2004. The requirements are of course intended to prevent the production and fielding of weapons systems that don't work [many of which have been the subject of discussion in RISKS in the past]. Last year, the Missile Defense Agency was already given managerial autonomy and removed procurement procedures that were intended to ensure new weapons programs remain on track and within budget. [From the RISKS perspective of having observed systems that do not work properly even with extensive oversight and testing, this seems like a very unwise approach.] [Source: Missile Defense Waiver Sought; White House wants to exempt the Pentagon's

controversial weapons system from operational testing rules, a first for a major program, by Esther Schrader, *Los Angeles Times*, 24 Feb 2003; PGN-ed]

<http://www.latimes.com/news/nationworld/nation/>

[la-na-missile24feb24,1,5024689.story?coll=la%2Dhome%2Dheadlines](http://www.latimes.com/news/nationworld/nation/la-na-missile24feb24,1,5024689.story?coll=la%2Dhome%2Dheadlines)

✶ "Bugsplat"--collateral damage simulator

"Daniel P.B. Smith" <dpbsmith@world.std.com>

Sat, 22 Feb 2003 09:48:12 -0500

[Best code name since "carnivore." DPBS]

US military planners hope to reduce the potential for civilian casualties in war by using a new computer program called Bugsplat. Instead of drawing concentric circles representing blast effects, Bugsplat generates blob-like images ("resembling squashed insects") that supposedly more precisely model expected damage. The hopes are that this program will help reduce collateral damage. QUOTE: "Because the program hasn't been used for actual targeting, this will be 'learn as you go.'" [Source: 'Bugsplat' program gives planners hope, By Bradley Graham, *The Washington Post*, 22 Feb 2003; PGN-ed]

✶ Scientology critic fined for undeclared file

Mark Thorson <eee@sonic.net>

Thu, 20 Feb 2003 19:06:41 -0800

A prominent French critic of Scientology has been fined 901 euros for maintaining a Web site that contained the name of a Scientologist in quotations from two published articles. The Scientologist sued, claiming his religious rights had been violated.

A 1978 French law intended to protect privacy requires computer files containing names of people (even one name) to be declared with the National Commission of Computers and Liberties (CNIL). On 18 Feb 2003, Roger Gonnet became the first person disciplined under this law for his Web site, <http://www.antisectes.net>, which has been operating since March 1997.

The judgment against Gonnet was 450 euros for violating the law, 450 euros for plaintiff's legal costs, and 1 euro for damages to plaintiff. (Plaintiff had been asking for 15,000 euros.)

Gonnet says, "At least 20 million French people are guilty of the same 'crime': they have individual names in their organizers, electronic agendas, computers, laptops, CD Roms, DVD roms, hard disks, memory cards, and even in their cell-phone memories, WAPs, texts, and Web sites, as well as the employers and commercial employees or sellers have lists of their employees, clients, associates, etc."

["What's In A Name?" Oui!
"What Name is In?" Non!!!
PGN]

✶ eBay: Big Brother is watching you, and documenting

Monty Solomon <monty@roscom.com>

Thu, 20 Feb 2003 17:34:28 -0500

"I don't know another Web site that has a privacy policy as flexible as eBay's," says Joseph Sullivan, director of the "law enforcement and compliance" department at eBay.com, reportedly the world's largest retailer. Sullivan was speaking to senior representatives of numerous law-enforcement agencies at "Cyber Crime 2003". His lecture was closed to reporters, but, in a recording obtained by Haaretz, Sullivan says that eBay is willing to hand over everything it knows about its Web users when asked by investigators. [Source: Yuval Dror, Haaretz; PGN-ed]
<http://www.haaretz.com/hasen/pages/ShArt.jhtml?itemNo=264863>

✶ Telepathy used to defend voting systems?

"Rebecca Mercuri" <notable@mindspring.com>

Tue, 28 Jan 2003 13:50:51 -0500

The Canadian Broadcasting Corp. reported that balloting at the 25 Jan 2003 NDP leadership convention in Toronto was disrupted by the SQL Slammer DDoS attack. The system that was being used was one provided by election.com -- one of the vendors also vying for Internet voting contracts in the USA.

Apparently election.com's Earl Hurd thought it was a laughing matter when he told the CBC: "Unless he died in the last few minutes because of the evil thoughts in my brain, he or she is still out there."

http://www.cbc.ca/cgi-bin/templates/print.cgi?/2003/01/25/ndp_delay030125

⚡ Voting machine engineer sues, alleges machine design flaws

<SusanMarieWeber@earthlink.com>

Sun, 23 Feb 2003 09:26:12 -0800 (PST)

Bev Harris, Black Box Voting <<http://www.blackboxvoting.com>>, 21 Feb 2003

Dan Spillane, a voting machine test engineer, filed a lawsuit against his former employer, DRE touch-screen voting machine manufacturer VoteHere.

Georgia recently approved VoteHere's machines, and the military is considering them for overseas voting. The company does business also in Sweden and England, and appears to be manufacturing, or planning to manufacture, components for other voting machine companies.

Spillane alleges in his lawsuit that he reported over 250 errors in the system, including critical errors of "severity 1" which include errors that may prevent the machines from correctly registering the votes. He sought meetings with company officials to express concerns about system integrity flaws, and created logs and reports of such flaws.

His complaint indicates that VoteHere did not address the flaws, and that the VoteHere system was certified by independent testing labs despite known flaws. Just when the testing lab began its examination of system integrity, VoteHere fired Spillane.

VoteHere's board of directors includes former CIA director Robert Gates.

VoteHere's Chairman is Admiral Bill Owens, who was senior military assistant to Secretaries of Defense Frank Carlucci and Dick Cheney. Carlucci, of course, now heads the Carlyle Group and Cheney is Vice President.

I will retrieve a copy of the lawsuit early next week, case # 03-2-18779-85SEA, filed in King County, Washington. If possible we will post it later in the week.

Bev Harris

🔥 Latest spam scam

Jim Griffith <griffith@dweeb.org>
Mon, 24 Feb 2003 21:10:21 -0500

I just received the following:

From: dlj4tbad5@hotmail.com (Former NetGaming Programmer)
Subject: Please help me

Hello dear friend,

I'm the developer who made the software for the NetGaming Casino.

But since they still did not paid me for last six month of work I decided

to reveal the backdoor in that casino I made for myself.

This backdoor allow easily win the roulette.

So: What do you need to win? Read below:

1. Go to the following secret link::

[http://www.\[deleted\]/?affiliate_id=230083&campaign_id=20016](http://www.[deleted]/?affiliate_id=230083&campaign_id=20016)

2. Open an account (click "Join Now").

3. Play roulette until "13" turn out. That's it! The next turn will be "27"!

I'll be happy if you ruin them by winning lots of money.

Either it's legitimate, in which case the Web site is totally screwed, or (far more likely) it's the most recent devious way to attract unsuspecting suckers.

🔥 Nigerian slain over e-mail scam

"John F. McMullen" <observer@westnet.com>

Sat, 22 Feb 2003 11:11:05 -0500 (EST)

Nigeria's consul in the Czech Republic, Michael Lekara Wayid, was shot and killed by a Czech citizen at the Nigerian Embassy in Prague on 19 Feb 2003.

The suspect had been victimized by a now-classical Nigerian scam, which resulted in the contents of his bank account vanishing.

[Source: Michelle Delio, Wired News; PGN-ed]

http://www.wired.com/news/culture/0,1284,57760,00.html?tw=wn_ascii

[This type of scam still seems to sucker in enough people to make it worth

the effort to keep the e-mail solicitations flowing. In the past week

alone, SpamAssassin has picked out 150 Nigerian scam spams in

my mailbox,
out of 2400 redirected spams; in the past two weeks, it has
trapped over
300 such scam spams addressed to RISKS, out of almost 1500
spams in all.
So it is definitely a booming industry. PGN]

✂ Spain - Vodafone sees its network crash after maintenance

Henry Baker <hbaker1@pipeline.com>
Fri, 21 Feb 2003 11:10:50 -0800

FYI -- 'Causative Maintenance' ?

Vodafone Spain's network virtually collapsed for almost 7 hours
on 21 Feb
2003, following what was thought to be basic maintenance work.
The company
has 8.7 million customers. No substantial explanation has been
given.

✂ An unexpected bill

Geoffrey Brent <g.brent@student.unsw.edu.au>
Sun, 23 Feb 2003 19:27:05 +1100

A friend of mine who is a postgraduate student at the University
of New
South Wales recently logged on to the university Web site to
check the fees
due for Semester 1, 2003. He was rather surprised to be told
that his debt
was slightly in excess of three million Australian dollars - by
a strange

coincidence, the sum owed was exactly equal to his student number.

Perhaps a little range-checking is in order?

✉ **Re: Surgeons transplant mismatched organs ([RISKS-22.58](#))**

K P <mrzeb@yahoo.com>

Mon, 24 Feb 2003 05:47:51 -0800 (PST)

Patients who need transplants are entered into the national transplant waiting list maintained by United Network for Organ Sharing (UNOS, Richmond VA) through a federal contract. The list includes many items including blood type, height and weight, how sick they are, and the hospital where they are waiting. Nationally, more than 80,000 people are waiting for hearts, lungs, kidneys, livers and pancreases.

When donor organs become available, information about blood type, size and location of the donor are entered into the computer generating a "match run" -- a list of all patients who are a medical match for that donor. They are listed in order of priority, determined by a complex calculation including components of illness and how near they are to the donor. A completed match run can range from tens of thousands to fewer than 10. Some organs are placed on the first call; others take hours.

According to news reports, in Jessica's case, Duke officials say transplant

coordinators called to offer the heart to two of their patients. The heart was the wrong size for one, and the other was not medically ready for a transplant. Jessica's doctor then asked about giving the heart and lungs to Jessica. Although she was not listed on the match run, the transplant coordinator said OK. Neither the coordinator nor the doctor realized that she was not the right blood type - the reason she was not on the computer's list of possible patients.

The UNOS systems didn't make the mistake. Humans intervened and ultimately caused the mistake.

It's sad that Jessica died as a result. But we will never know who else died because they didn't get the organs they should have in the first place.

[Dan Graifer noted that lengthy articles appeared in *The Washington Post*.

PGN]

<http://www.washingtonpost.com/wp-dyn/articles/A56656-2003Feb24.html>

<http://www.washingtonpost.com/wp-dyn/articles/A2700-2003Feb25.html>

🔥 Re: Deadly input validation? (Adams, [RISKS-22.58](#))

"Ed Ravin" <eravin@panix.com>

Sun, 23 Feb 2003 12:42:37 -0500 (EST)

[Although the original item was only marginally computer-related,

we include this item to correct the archival record. PGN]

Some corrections and clarifications:

* It was four teenagers in the rowboat, not two.

* The phone call from the distressed teenagers lasted about 12 seconds --
the 911 operator only heard that they were in a boat on Long Island Sound
and were taking in water before the call was cut off.

* The correct thing for the 911 operator to have done was to have assigned
the call to the police harbor unit. The operator did not know this
information, so he or she went to the supervisor for guidance.

* All supervisors had previously received a notice clarifying what to do
with marine distress calls -- but this supervisor apparently had forgotten
about that and also didn't know what to do with the call.

* The supervisor is getting departmental charges, and could be demoted
or dismissed. The operator received a "letter of instruction" but
was not otherwise disciplined.

* The cops claim that even if the harbor unit had been notified in time,
with the scant amount of information available it was unlikely they would
have found the boys in time.

More details at:

<http://www.nynewsday.com/news/local/wire/ny-bc-ny--missingteens0218feb18.story>

And no doubt in other NYC-area daily newspapers.

Despite what the cops say, things might have been different if they had properly logged the call - for example, the calling number for the cell phone should have been recorded, and had the police looked for the owner of the cell phone they might have been able to find one of the boys' parents and gotten a better idea of what was going on. However, given that the call was received on a frigid January evening, there probably wasn't much else that could be done until the next morning.

⚡ **REVIEW: "Building Secure Wireless Networks with 802.11", Khan/Khwaja**

Rob Slade <rslade@sprint.ca>
Tue, 25 Feb 2003 07:47:39 -0800

BKBSWNW8.RVW 20030208

"Building Secure Wireless Networks with 802.11", Jahanzeb Khan/
Anis

Khwaja, 2003, 0-471-23715-9, U\$40.00/C\$62.95/UK#29.95

%A Jahanzeb Khan

%A Anis Khwaja

%C 5353 Dundas Street West, 4th Floor, Etobicoke, ON M9B 6H8

%D 2003

%G 0-471-23715-9

%I John Wiley & Sons, Inc.

%O U\$40.00/C\$62.95/UK#29.95 416-236-4433 fax: 416-236-4448

%O <http://www.amazon.com/exec/obidos/ASIN/0471237159/>

[robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/0471237159/robsladesinterne)

<http://www.amazon.co.uk/exec/obidos/ASIN/0471237159/>

[robsladesinte-21](http://www.amazon.co.uk/exec/obidos/ASIN/0471237159/robsladesinte-21)

%O <http://www.amazon.ca/exec/obidos/ASIN/0471237159/>

[robsladesin03-20](http://www.amazon.ca/exec/obidos/ASIN/0471237159/robsladesin03-20)

%P 330 p.

%T "Building Secure Wireless Networks with 802.11"

As with any hot topic, there are lots of people willing (eager!) to tell you about the security of wireless local area networks, without first making sure that they really know the subject.

Part one is an introduction to wireless LANs. Chapter one is a history of networks, an outline of topologies (concentrating on cabling, interestingly enough), and a review of the TCP/IP (actually OSI, [Open Systems Interconnection] protocol stack. The last page gives too little information for an exercise in setting up a home LAN. Terms in regard to wireless technology are listed in chapter two, but the material is verbose without being informative. The explanations given for spectrum multiplexing are unclear, and seem to be delivered by rote without any understanding. The discussion does not build on that from chapter one to, for example, point out that ad hoc wireless networks are similar to bus topologies, while infrastructure networks are more akin to stars. The various IEEE (Institute of Electrical and Electronics Engineers) 802.11 standards are listed in chapter three. However, there is a great deal of material repeated from prior text (the discussion of spectrum is reprised almost word for word), and, other than some frequency and maximum bandwidth information, there is little additional detail. (Repetition and duplication is rife throughout the book, as well as a good deal of space wasted with pointless figures and graphics. On page 125 we are told that "The 40-bit shared key

is concatenated with a 24-bit long initialization vector" and referred to figure 6.1. Figure 6.1 tells us "Concatenated-Key = Shared-Key + IV." Not very helpful.) Chapter four is supposed to help you decide whether a wireless LAN is right for you, but only has some vague opining, a little content on wireless ISPs (Internet Service Providers: hardly suitable for LAN discussions), and almost no analysis or details.

Part two purports to emphasize secure wireless LANs. Chapter five has random topics regarding network security. Most of it is irrelevant to the specific needs of wireless situations or is not discussed in terms of the particular needs of wireless networks. (Physically securing the components of a wireless LAN has some importance in overall security, but may be pointless if someone driving by can take over the network). Securing the IEEE 802.11 wireless LAN is not reviewed well in chapter six. There is more duplication of content, few details about WEP (Wired Equivalent Privacy), and some clear evidence of misunderstanding of the base technologies. (If you are going to talk about 40 bit keys at the low level, higher level security should be 104, rather than 128, bit. And a 128 bit key is *not* equivalent to 64 characters, in anybody's representation.) When security aspects are discussed, often they relate to issues that are beyond the control of the user, such as moderation of signal strength.

Part three collects topics related to the building of secure wireless LANs.

Chapter seven is a simplistic overview of generic LAN planning. Shopping for the right equipment is important, but the list of product specifications in chapter eight fails to address vital areas, such as driver availability, default key length, and the existence of default accounts. More space is devoted to where you can buy equipment than how to evaluate it. The installation instructions, in chapter nine, pretty much ignore security considerations. Chapter ten supposedly deals with advanced wireless LANs, including security, but has little new material aside from screenshots of Microsoft Windows utilities with some relationship to VPNs (Virtual Private Networks).

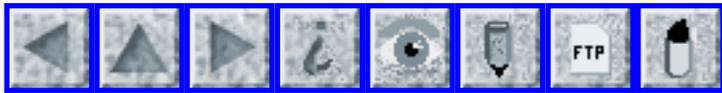
Part four covers troubleshooting and maintenance. Chapter eleven touches on a number of possibly wireless connectivity problems. A collection of text repeated from prior chapters is in chapter twelve.

There is a glossary included with the book. It is quite limited, and, in particular, does not deal well with acronyms. In fact, the book is full of TLAs (Three Letter Acronyms) and other abbreviations that get used before they are defined, and do not appear in either the glossary or the index. This can be quite aggravating, particularly in cases where the acronyms aren't standard. (The authors use "PHY" to refer to the physical layer of the OSI model, which is not commonly so represented in either communications or security literature.)

The text of the book is excessively padded with useless verbiage

and irrelevant material. The actual content pertinent to the security of wireless LANs is barely enough to fill a decent magazine article. Overall, the book is poorly structured, limited in detail, and bloated with meaningless or repetitious content.

copyright, Robert M. Slade, 2003 BKBSWNW8.RVW 20030208



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

[ACM](#) Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 60

Monday 3 March 2003

Contents

- [Reversed 2002 election results in Alabama still unexplained](#)
[PGN](#)
- [Computer error grounds Japanese flights](#)
[Eric De Mund](#)
- [Japanese bullet trains still don't have dead-man switches](#)
[Joyce Scrivner](#)
- [Electronically controlled failure of operating table](#)
[Patrik Reali](#)
- [50,000 court records erased](#)
[David Kipping](#)
- [Fake job listings on Net fostering identity theft](#)
[PGN](#)
- [*Big* Red faces at Cornell over e-mail error](#)
[PGN](#)
- [How to spam a closed mailing list](#)
[Andrew Lynch](#)
- [New telemarketing tool makes caller ID fakery easy](#)
[Mathew](#)
- [Lexmark wins injunction in DMCA case](#)
[David Becker via Monty Solomon](#)

- [BSA Accuses OpenOffice ftp sites of piracy](#)
[Michael Weishaar](#)
 - [FCW: Group issues final biometrics report](#)
[PGN](#)
 - [Someone protecting patient data well](#)
[Richard A. O'Keefe](#)
 - [Error: Scientology critic fined for undeclared file](#)
[Roger Gonnet](#)
 - [REVIEW: "WiFi Security", Stewart S. Miller](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ **Reversed 2002 election results in Alabama still unexplained**

"Peter G. Neumann" <neumann@csl.sri.com>

Thu, 27 Feb 2003 17:01:47 PST

[Thanks to Kim Alexander <kimalex@calvoter.org> for noting this item.]

The Alabama governor's election in Nov 2002 was irrevocably impeded by an unexplained anomaly in the use of ES&S optical-scan voting equipment in Baldwin County, which reversed the outcome of the election. In this case, the printed results of votes produced in the Magnolia Springs precinct were accurate (when compared with the actual ballots), but the data on the cartridges used to tabulate the final results electronically was seriously in error. Unfortunately for the candidate who should have won based on the acknowledged correct results, the erroneous electronic totals (in which about 6,300 votes for that candidate were missing) were accepted as

official. The official loser "ultimately abandoned his challenge after it became clear that he would not be able to get the statewide vote recount he had sought." Thus, the candidate with the most votes was declared the loser. Three months after the election, it is still unclear why the cassette was missing so many votes disappeared, blamed on a "computer glitch" -- possibly a "power surge at the precinct, static electricity, or something else". [Source: Brendan Kirby, Voting snafu answers elusive, *The Mobile Register*, 28 Jan 2003; PGN-ed]

http://www.al.com/news/mobileregister/index.ssf?/xml/story.ssf/html_standard.xsl?/base/news/104374962627050.xml

This case in Alabama is just one more example of why incontrovertible audit trails are essential -- especially when electronic results can so easily be either accidentally incorrect or fraudulently tampered. In the even less perspicuous case of all-electronic elections, a voter-verified ballot image is ever-more essential. See an article by Henry Norr in today's *San Francisco Chronicle*

<http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2003/03/03/BU122767.DTL&type=tech>

as well as David Dill's Web site and petition at

<http://verify.stanford.edu/evote.html>

and Rebecca Mercuri's Web site

<http://www.notablesoftware.com/evote.html>

plus the many items in previous issues of RISKS relating to the general problem of election integrity and accountability. This kind of problem is really getting out of hand, and deserves your closer attention.

(If you cannot find the *Chron* column, I put a copy up on my Web site:

<http://www.csl.sri.com/neumann>)

PGN

[Date typo fixed in archive copy. PGN]

✂ Computer error grounds Japanese flights

Eric De Mund <ead@ixian.com>

Sun, 2 Mar 2003 21:11:10 -0800 (PST)

As seen on Slashdot. [http](http://www.slashdot.org) URLs verified (9:00pm PST, 02 Mar 2003):

Computer Error Grounds Japanese Flights

<http://slashdot.org/article.pl?sid=03/03/02/2123253>

Posted by timothy[1] on Sunday March 02, @04:50PM
from the presumption-junction dept.

zephiros[2] writes "Mainichi Daily News reports[3] that a "computer glitch" in Tokyo air traffic control systems resulted in the cancellation of 203 flights this weekend. At 7am Saturday, the error "caused the names of airlines and flight numbers to disappear from radar screens." A Japan Times[4] article suggests the problem may be related to upgrades on a system which exchanges flight plans with the Defense Agency. Makes one wonder about the integration and maintenance risks of systems like CAPPS II [5]."

Quote from [3]:

"Computers are just no good," said one 51-year-old company

manager

leaving [from Nagoya airport] for Sapporo. "I'm sure they're helpful, but they're just too fragile."

Excerpt from [4]:

The troubled flight data-processing system at the ministry's [6] Tokyo Air Traffic Control Center in Tokorozawa, Saitama Prefecture, automatically transmits flight information to airports across Japan. The system manages flight plans.

The ministry said that early Saturday it partially replaced programs in the system that exchanges flight plans with the Defense Agency. The system went down immediately after it was turned on following the replacement.

A transport ministry official said it was too early to link the change to the failure.

The air traffic center was forced to take alternative measures, which included telephoning airports to give flight information and inputting flight data manually.

The system has a backup, but both systems went down at the same time, according to the ministry.

Notes:

1. <http://www.monkey.org/~timothy/>
2. <mailto:joseph%20at%20dreamlands.org>
3. <http://mdn.mainichi.co.jp/news/archive/200303/01/20030301p2a00m0dm002000c.html>
4. <http://www.japantimes.co.jp/cgi-bin/getarticle.pl5?nn20030302a1.htm>

5. <http://www.privacyactivism.org/Item/48>

6. Land, Infrastructure and Transport Ministry at Tokyo's Haneda airport

Eric De Mund <ead@ixian.com> Ixian Systems, Inc. Mountain View, CA
<http://www.ixian.com/ead/>

[Also noted by David Kennedy, Naoki Yamamoto, and Bob Heuman -- who added:

"The risks should be obvious, even if the cost in this instance is

not. How many times will we hear 'due to a reprogramming hiccup' and

why were both the main system and the backup taken out of service???

It is interesting how the press sensationalised it by throwing in

security preparedness and nuclear arms, which are NOT direct risks from

this incident."

PGN]

⚡ Japanese bullet trains still don't have dead-man switches

joyce scrivner <kscriv@earthlink.net>

Thu, 27 Feb 2003 07:01:33 -0600

A couple years ago, in [RISKS-21.27](#), I noted a bullet train that ran without

a driver. This new item shows the driver can fall asleep and the train

keeps running. It stopped, but not before timing out.

A bullet-train driver snoozed at the wheel for 8 minutes on 26 Feb 2003

while the high-speed train ran at a speed of 270 kilometers per hour.

Fortunately, because the driver had failed to push a confirmation button and apply the brakes manually, an automatic brake system stopped the train at the wrong location -- 100 meters short of the Okayama Station on the West Japan Railway. Station workers found the drivers still asleep, as he had been ever since the Shin-Kurashiki Station. [Source: *Mainichi Shimbun*, 27 Feb 2003; PGN-ed]
<http://mdn.mainichi.co.jp/news/20030227p2a00m0fp001000c.html>

✶ Electronically controlled failure of operating table

"Patrik Reali" <reali@acm.org>
Sun, 2 Mar 2003 10:33:33 +0100

An article notes unexpected troubles while doing heart surgery at Derriford Hospital in Plymouth. During the surgery, an electronically controlled operating table ("an up-to-date 50,000-pound [money, not weight] piece of equipment") began collapsing, causing the patient to "jolt forward". The patient died three days later, but there is no evidence the two events are correlated.....

<http://www.timesonline.co.uk/article/0,,2-593995,00.html>

✶ 50,000 court records erased

"David Kipping" <dkipping@mindspring.com>
Thu, 27 Feb 2003 12:03:55 -0700

A computer crash has erased nearly 50,000 local 3rd District Court cases ... in southwestern Idaho [Caldwell]. ... Third District Court Administrator Dan Kessler said staff members arrived Tuesday to learn the court's computer server dumped thousands of new court cases and countless updates to older ones. ... "It's more than a mere glitch," Kessler said. "We lost all of our database from March 5, 2002 to Feb 14, 2003." [A lot of discussion of how difficult it is to conduct business without the records.] ... John Peay, information systems chief for the Idaho Supreme Court said his office is to blame for an operator error when a technician was expanding the 3rd District court computer to improve response time. As a result, both copies of the records were lost. The hard drive was sent to California, where specialists may be able to recover some of the lost data. [Excerpt from AP story, 20 Feb 2003]

[As I read this, the backup was a duplicate copy of the data on the server hard disk. Apparently there was no other backup -- tape, CD, other server, etc. The RISKS are obvious. DK]

🔥 Fake job listings on Net fostering identity theft

"Peter G. Neumann" <neumann@csl.sri.com>
Fri, 28 Feb 2003 19:11:40 -0800 (PST)

Monster.com (which claims to house 24.5 million resumes) sent out a "critical service message" to millions of job seekers, warning that bogus job postings are resulting in the illegal collection of personal information that could result in identity theft. This is a problem that applies equally to CareerBuilder.com, HotJobs.com, and other job sites as well, although these others seem to be downplaying the risks.

<http://www.cnn.com/2003/TECH/internet/02/28/monster.theft.ap/index.html>

***Big* Red faces at Cornell over e-mail error**

Peter Neumann <Neumann@CSL.sri.com>

Fri, 28 Feb 2003 10:38:02 -0500

Cornell University sent e-mail to 1,700 high-school students on 26 Feb 2003 informing them that they had been accepted into the class of 2007. However, almost 550 of these students had previously been informed in Dec 2003 that they had been rejected. Shortly thereafter, the mistake was recognized, and followed by an "oops" e-mail, apologizing for the error. [Source: Karen W. Arenson, *The New York Times*, 28 Feb 2003; PGN-ed]

<http://www.nytimes.com/2003/02/28/education/28CORN.html>

***How to spam a closed mailing list**

"Andrew Lynch" <andrew.lynch@knuut.de>

Sat, 1 Mar 2003 15:55:44 +0100

As a member of ACM SIGOPS, I am on their sigops-announce mailing list. Just now I received e-mail from that list with the subject "Rejected posting to SIGOPS-ANNOUNCE@ACM.ORG", even though I have never posted to this list.

The rejected mail claimed to be from sigops-announce@listserv.acm.org itself, but with an IP address that does not match my DNS server's entry for listserv.acm.org.

The rejected mail was included in full and consisted of some HTML code with an IFRAME-embedded attachment containing a file named README.EXE disguised as Content-Type audio/x-wav. Luckily my Unix mail program does not interpret HTML. I hate to think what this might do in MS-Outlook and friends.

The risk resulted from a combination of two things:

- (a) The (automatic?) rejection message from the list server contains a complete copy of the original mail.
- (b) The original sender fakes his address to be that of the list itself.

The result is that the list server happily sends the rejected message to the whole list (albeit with a different subject line).

⚡ New telemarketing tool makes caller ID fakery easy

mathew <meta@pobox.com>

Thu, 27 Feb 2003 20:31:16 -0500

Castel Inc., a maker of automated dialing technology, boasts that its

DirectQuest software is immune to the TeleZapper, a \$40 gadget designed to

thwart sales calls by faking the tones of a disconnected number.

Beverly, Mass.-based Castel has been mailing brochures to telemarketers

and other prospective customers touting the software, which also includes

a feature that lets salesmen transmit any phone number or text message to

residents' caller ID displays.

http://story.news.yahoo.com/news?tmpl=story&ncid=528&e=5&cid=528&u=/ap/20030226/ap_on_hi_te/telemarketer_tool

Obviously, no regular RISKS reader trusts caller ID at this point. However,

I suspect that enterprising criminals who purchase this \$2,700 caller-ID-faking equipment will get a healthy return on investment.

✶ Lexmark wins injunction in DMCA case

Monty Solomon <monty@roscom.com>

Thu, 27 Feb 2003 23:51:07 -0500

Printer maker Lexmark International Group won a preliminary injunction on 27

Feb 2003 in efforts to prevent a company from selling computer chips that

allow toner cartridges to be recycled. Judge Karl Forester of the U.S. District Court for the Eastern District of Kentucky issued the pretrial injunction against Static Control Components, a small Sanford, N. C.-based company that sells printer parts and other business supplies. The order prohibits the company from selling its Smartek chip. When installed in compatible Lexmark printers, the chips allow the printers to use cheaper recycled toner cartridges that would otherwise be rejected by the printer's sensors. [Source: David Becker, CNET News.com, 27 Feb 2003] <http://news.com.com/2100-1028-990501.html>

BSA Accuses OpenOffice ftp sites of piracy

<michael.weishaar@earthlink.net>

Fri, 28 Feb 2003 08:57:38 -0600 (CST)

It seems that some FTP sites that host OpenOffice are getting "cease and desist" e-mail from the BSA about their purported piracy of MS Office.

Maybe their scripts should enhance their search criteria.

Imagine the

consequences if the BSA (or some other IP watchdog) had the authority to shut down "piracy" sites.

[Maybe a browser string search on "MS" and "OFFICE" also results in women

being asked to cease and desist if they are referred to as "MS." and

happen to have the title "Corporate Executive OFFICEr". PGN]

Here is an excerpt of the e-mail, which was posted at <http://distribution.openoffice.org/servlets/ReadMsg?msgId=581265&listName=dev>

```
>> From: "Copyright Europe" <copyright-europe@bsa.org>
>> To: "Abuse" <network@uni-muenster.de>
>> Sent: Wednesday, February 26, 2003 5:51 PM
>> Subject: [NOC] Case ID 588853 - Notice of Claimed Infringement
>>
>> Wednesday, February 26, 2003
>>
>> Westfaelische Wilhelms - Universitaet
>> Roentgenstr. 9-13
>> Muenster, D-48149 DE DE
>>
>> Re: Unauthorized Distribution of the following copyrighted
computer
>> program(s):
>>
>> Microsoft Office
>>
>> Dear Sir/Madam:
>>
>> The Business Software Alliance (BSA) has determined that the
connection
>> listed below, which appears to be using an Internet account
under your
>> control, is operating an FTP server to offer unlicensed
copies or is
>> engaged in other unauthorized activities relating to
copyrighted computer
>> programs published by the BSA's member companies.
>>
>> Infringement Details:
>> -----
>> First Found: 24 Nov 2002 15:31:40 EST (GMT -500)
>> Last Found: 24 Feb 2003 01:19:59 EST (GMT -500)
>> IP Address: 128.176.191.21
>> IP Port: 21
>> Protocol: FTP
>> FTP Login Name: anonymous
>> FTP Login Password: guest@nowhere.com
>>
```

>> What was located as infringing content:
>> -----
>> Filename: /mandrake_current/SRPMS/OpenOffice.org-1.0.1-9mdk.
src.rpm
>> (199,643kb)
>> Filename:
>>
>> /mandrake_current/i586/Mandrake/RPMS/OpenOffice.org-libs-1.0.1-
9mdk.i586.rpm
>> (35,444kb)
>>
>> The above computer program(s) is/are being made available for
copying,
>> through downloading, at the above location without
authorization from
>> the copyright owner(s).
>>
>> Based upon BSA's representation of the copyright owners in
anti-piracy
>> matters, we have a good faith belief that none of the
materials or
>> activities listed above have been authorized by the
rightholders, their
>> agents, or the law. BSA represents that the information in
this
>> notification is accurate and states, under penalty of
perjury, that it
>> is authorized to act in this matter on behalf of the
copyright owners
>> listed above.
>>
>> We hereby give notice of these activities to you and request
that you
>> take expeditious action to remove or disable access to the
materials
>> described above, and thereby prevent the illegal reproduction
and
>> distribution of pirated software via your company's network.
As you
>> know, illegal on-line activities can result in 50 million
people on
>> the Internet accessing and downloading a copyrighted product
worldwide

>> without authorization - a highly damaging activity for the
copyright holder.
>>
>> We appreciate your cooperation in this matter. Please advise
us
>> regarding what actions you take.
>>
>> Please include the following CaseID in any response you send:
Case ID
>> 588853
>>
>> Yours sincerely,
>>
>> Corinna Beck
>> Business Software Alliance
>> 1150 18th St NW Suite 700
>> Washington,DC 20036
>> <http://www.bsa.org>
>> E-mail: copyright-europe@bsa.org

✶FCW: Group issues final biometrics report

"Peter G. Neumann" <neumann@csl.sri.com>

Thu, 27 Feb 2003 15:41:15 PST

[Source: Group issues final biometrics report Michael Hardy,
*Federal
Computer Week*, 25 Feb 2003; PGN-ed]

The International Biometric Group has presented the White House's Office of Science and Technology Policy with a 200-page final report on using biometric technologies to secure the nation's borders, airports, and seaports. New counterterrorism laws, including the USA Patriot Act and Enhanced Border Security and Visa Entry Reform Act, require

authorities to
use biometrics to detect immigration fraud.

Among the report's recommendations:

* The United States should design a solution that incorporates other

countries' choices of biometrics. The United States, for example, may

prefer fingerprint readers because they can interact with existing law

enforcement databases, while another country chooses facial recognition or

iris scanners.

* The State Department should capture multiple biometric identifiers from

every person who applies for a U.S. visa, including high-quality face,

fingerprint and iris scans.

* Biometrics used at a port of entry should augment, not replace, an

inspector's judgment in deciding whether to admit someone.

* Use tethered portable fingerprint devices in traffic lanes at border

crossings to easily read fingerprints from everyone in a car.

In a similar study recently, the Commerce Department's National Institute of

Standards and Technology suggested that a combination of fingerprint and

facial-recognition technologies would be the most secure. NIST suggested

using at least two fingerprints to identify each visa applicant, and a

combination of fingerprint and facial recognition to verify the identity of

visa holders crossing borders.

[The GAO also has a report on the relative merits of using biometrics

for border security, GAO-03-174, Nov 2002. PGN]

Someone protecting patient data well

"Dr Richard A. O'Keefe" <ok@cs.otago.ac.nz>

Fri, 28 Feb 2003 16:20:24 +1300

We hear so much bad news on comp.risks I thought it would be nice to pass on a story about someone doing something right. A common mistake is selling computers whose discs contain sensitive information. There's a medical research group in this University that get data from all round the country, including patient name, address, phone number, and all sorts of stuff. I asked the sysadmin what she did when they disposed of any computers.

1. The disc is reformatted.
2. The drive is physically removed from the computer.
3. The case of the drive is opened, and every visible wire cut.
4. She then takes it home and her husband slams a heavy axe through the platter a couple of times.
5. The thing is then put in an ash bucket and hot domestic ash dumped on it and shaken well in.
6. Finally it's taken to the recycling depot.

If there's anything she can do to make it harder for the data to be recovered, short of melting the unit down, I'd like to know what it might be, and so would she.

✂ Error: Scientology critic fined for undeclared file ([RISKS-22.59](#))

"roger gonnet" <gonnet@antisectes.net>

Sat, 1 Mar 2003 08:40:05 +0100

The item in [RISKS-22.59](#) is erroneous; indeed, the "religious" aspect wasn't part of the final trial against me. Though the plaintiff tried to complain also for that (Article 226-19 of the penal code), this was specifically dismissed by the instructor judge (Non-lieu).

The truth of the matter is that in France, Article 226-16 of the penal code (for which I was convicted) says that one has no right to establish any lists of people's names before having done some "declaration of personal filings" to an official agency (called CNIL).

Another Article (226-19) establishes a rule about an interdiction to file religious and political opinions of people, but I wasn't sued for that, because Scientology is considered to be a dangerous cult in France, and has never been called a religion apart from a sentence by a judge that was subsequently canceled by the Supreme Court (Cassation).

Moreover, the State Council has even rejected the religious status of Scientology years ago, and the cult does pay lots of taxes, like companies.

[Slight changes made in English for clarity, hopefully without changing

the intended meaning. I trust Roger will correct me if I erred. Merci!

PGN]

REVIEW: "WiFi Security", Stewart S. Miller

Rob Slade <rslade@sprint.ca>

Thu, 27 Feb 2003 07:46:34 -0800

BKWIFISC.RVW 20030209

"WiFi Security", Stewart S. Miller, 2003, 0-07-141073-2,
U\$49.95/C\$78.95/UK#40.00

%A Stewart S. Miller wifi@itmaven.com

%C 300 Water Street, Whitby, Ontario L1N 9B6

%D 2003

%G 0-07-141073-2

%I McGraw-Hill Ryerson/Osborne

%O U\$49.95/C\$78.95/UK#40.00 800-565-5758 fax: 905-430-5020

%O <http://www.amazon.com/exec/obidos/ASIN/0071410732/>

[robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/0071410732/)

<http://www.amazon.co.uk/exec/obidos/ASIN/0071410732/>

[robsladesinte-21](http://www.amazon.co.uk/exec/obidos/ASIN/0071410732/)

%O <http://www.amazon.ca/exec/obidos/ASIN/0071410732/>

[robsladesin03-20](http://www.amazon.ca/exec/obidos/ASIN/0071410732/)

%P 309 p.

%T "WiFi Security"

When a book starts out with a preface that is basically an advertising pitch for the author's consulting services, one can be forgiven for doubting the author's dedication to the task of informing the audience. This work is yet another attempt to jump on a hot topic bandwagon.

Supposedly chapter one introduces us to the standards for wireless LAN security. Instead, the material meanders through an unstructured collection of security and wireless topics. The material is limited,

random, and not particularly informative. Even when dealing with strictly technical areas, such as the various types of spread spectrum technologies, the text seems to have been lifted wholesale from marketing brochures, and fails to explain much of anything. There isn't much "Technology Comparison" in chapter two unless we are comparing apples and oranges: again there is a haphazard compilation of topics, with Bluetooth getting the lion's share of the ink. Instead of considering security factors, chapter three lists some basic attacks against systems in general. The "issues in wireless security" are a little more on topic in chapter four.

Chapter five mentions a few terms related to the 802.11 family of standards. There isn't much about the promised 802.11 security infrastructure in chapter six: instead we have another amalgam of security problems. Miller demonstrates his limited understanding of the technology, in chapter seven, with common mistakes such as the comparison of "40" and "128" bit WEP (Wired Equivalent Privacy) keys (WEP keys are composed of either 40 or 104 bit base keys concatenated with 24 bit initialization vectors, for total lengths of 64 or 128 bits respectively), so it is no surprise that the analysis of the weaknesses of WEP is only half a page long, and misses all the fundamental problems.

Chapter eight is a generic warning that people might snoop on you. The authentication topics jump around so much that it is impossible to say what

chapter nine is really talking about. A number of technologies are mentioned, but those discussed together frequently come from completely separate protocols or functions. Similarly, chapter ten is entitled "Direct Sequence Spread Spectrum," but doesn't explain anything about DSSS at all, and isn't even consistent in terms of the subject area under discussion. Chapter eleven does stick to the topic of equipment issues, but does not provide any useful direction to the reader. Cross-platform issues are rather confused, in chapter twelve, although there is a reasonable discussion of the WEP initialization vector reuse problem--which should have been covered in chapter seven. The vulnerabilities listed in chapter thirteen constitute another grab bag: since we have been discussing wireless LANs throughout the book, why do we now bring up the topic of the "WAP (Wireless Access Protocol) gap," which only affects Internet enabled cell phones? Chapter fourteen and fifteen mostly duplicate content from nine, with a few minor additions. Chapter sixteen repeats a lot of other material, adding a tiny bit on risk assessment. PDA security issues are reviewed in chapter seventeen. Chapter eighteen collects another random assortment of duplicated topics for a supposed look to the future.

This is an arbitrary and disorganized conflation of subjects, with very little of value to anyone. There are a few salient and helpful facts, which, if brought together, might fill a few pages. However, these tidbits

are buried in a deluge of impenetrable verbiage, designed more to impress the naive reader than to inform anyone.

copyright, Robert M. Slade, 2003 BkWIFISC.RVW 20030209



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

[ACM](#) Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 61

Thursday 6 March 2003

Contents

- [Slight change in RISKS e-mail procedure](#)
[RISKS List Owner](#)
- [Computer error means 2.3-trillion-pound electricity bill](#)
[Fuzzy Gorilla](#)
- [Computer error halts fuel payments](#)
[Fuzzy Gorilla](#)
- [Indiana University Center's computers breached by hacker](#)
[Sheri Alpert](#)
- [Risks of using Tax IDs for other things](#)
[Peter Wayner](#)
- [28 Krispy Kreme customers each charged over \\$84,000](#)
[Fuzzy Gorilla](#)
- [Visa moves to improve customers' privacy](#)
[PGN](#)
- [Credit-card fraud](#)
[Thomas Kristmar](#)
- [Credit company's customer list leaked to an underground gang](#)
[Chiaki Ishikawa](#)
- [16M Yen stolen from sniffed bank passwords at Internet Cafe](#)
[Chiaki Ishikawa](#)

- [Wrongly jailed woman blames system](#)
[Fuzzy Gorilla](#)
 - [Re: Reversed 2002 election results in Alabama still unexplained](#)
[Dale Pennington](#)
[PGN](#)
 - [Re: Computer error grounds Japanese flights](#)
[Chiaki Ishikawa](#)
 - [Re: BSA Accuses OpenOffice ftp sites of piracy](#)
[Fritz Whittington](#)
 - [New IEEE Security and Privacy magazine](#)
[Gary McGraw](#)
 - [REVIEW: "Security in Computing", Charles Pfleeger/Shari Pfleeger](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ Slight change in RISKS e-mail procedure

RISKS List Owner <risiko@csl.sri.com>

Thu, 6 Mar 2003 10:48:55 PST

Although it should be largely invisible to you, this issue is being sent out in a way that should dramatically simplify our processing of the steadily large number of e-mail bounces (including unresolvable black-hole bounces for no-longer-existing mail exchangers). This will enable us to more easily cull out the offending addresses. We will still be very conservative in not removing temporarily offending addresses. Please let us know if you find yourself inadvertently no longer receiving RISKS. Many thanks to Mike Hogsett, who has been superb in putting up with the strain that RISKS puts on our e-mail servers.

⚡ Computer error means 2.3-trillion-pound electricity bill

"Fuzzy Gorilla" <fuzzygorilla@euroseek.com>

Tue, 04 Mar 2003 18:35:36 -0500

The **Yorkshire Post** reports that after a man had forgotten to pay an earlier electricity bill of 59 pounds from British Gas for a house in Fartown, Huddersfield, he received a final demand for 2,320,333,681,613 pounds. After he was threatened with court action, the local media intervened. At that point, British Gas admitted there had been a mistake, ``with a computer mixing up the reference number for the property.'' On the other hand, a BG spokeswoman was quoted as saying that it was a ``simple clerical mistake''. [PGN-ed]
http://www.ananova.com/news/story/sm_756911.html

⚡ Computer error halts fuel payments

"Fuzzy Gorilla" <fuzzygorilla@euroseek.com>

Tue, 04 Mar 2003 18:41:51 -0500

1,128 people over 60 are still waiting for their 200-pound winter fuel payments, two months after they should have been paid. The Department for Work and Pensions (DWP) told the BBC that the computer system which handles

payments has 'lost' their records, and that they would have to trace back to the original applications. [Source: BBC, Money Box, Paul Lewis, 18 Feb 2003; PGN-ed]
<http://news.bbc.co.uk/1/hi/programmes/moneybox/2764451.stm>

Indiana University Center's computers breached by hacker

Sheri Alpert <salpert@nd.edu>
Wed, 5 Mar 2003 14:54:01 -0500 (EST)

[Source: Article by Terry Horne <terry.horne@indystar.com>, telephone 1-317-444-6082, *The Indianapolis Star*, 28 Feb 2003; PGN-ed]
<http://www.indystar.com/print/articles/3/025875-2223-P.html>
(another story at: <http://www.sagamore.iupui.edu/32/32-24/24hacker.html>)

About 7,000 patients of the Indiana University Center for Sleep Disorders have had the confidentiality of their Social Security numbers and other personal information compromised by a hacker who broke into the center's computer on 27 Nov 2002, although it was not discovered until 3 Jan 2003. Reportedly, there is no evidence any identities were stolen or even that files were offloaded. Intent had apparently to use this computer system as a bridge to other university computers.

[This intrusion might have caused some additional sleep disorders after the patients were notified. PGN]

✶ Risks of using Tax IDs for other things

Peter Wayner <pcw@flyzone.com>

Thu, 6 Mar 2003 14:03:55 -0500

A Princeton student tried PNC's new Internet banking Web site to check his student organization's funds and found he could access *all* of the university's accounts holding almost \$10 million in total. The student organization used the same taxpayer ID number as the rest of the university, and the bank's Web site used the ID to link the records.

[http://story.news.yahoo.com/news
?tmpl=story2&cid=816&ncid=816&e=5&u=/ap/20030306/ap_on_fe_st/
banking_glitch](http://story.news.yahoo.com/news?tmpl=story2&cid=816&ncid=816&e=5&u=/ap/20030306/ap_on_fe_st/banking_glitch)

✶ 28 Krispy Kreme customers each charged over \$84,000

"Fuzzy Gorilla" <fuzzygorilla@euroseek.com>

Tue, 04 Mar 2003 19:31:54 -0500

A Krispy Kreme doughnut shop in Albuquerque seemingly greased its coffers while figuratively deep-frying over two dozen customers. Irrespective of what they ordered, each of 28 customers using a credit card were charged EXACTLY \$84,213.60 for the purchase. KK blamed Heartland Payment Systems, which processes their credit-card transactions. [Source: KRQE News 13, Albuquerque, N.M., 19 Feb 2003; PGN-ed]

<http://www.krqe.com/Global/story.asp?S=1140274>

[These charges were actually APPROVED, and of course also blew the customers' credit ratings for a few days. Amazing! ``The \$84,000 charge, were it legitimate, would have purchased over 170,000 ... doughnuts, enough to stretch over 9 miles if placed end-to-end.''
(But a few days later, the doughnuts might have settled into substantial paving bricks. Or do Krispy Kremes have a shelf-life of years, like the bread and chocolate used in Desert Shield?) Of course, stacked vertically, they would reach almost 2 miles high. Somehow, the name ``Heartland'' seems incompatible with the concept of Krispy Kremes, unless it is related to a hospital with the same name.
PGN]

✶ Visa moves to improve customers' privacy

"Peter G. Neumann" <neumann@CSL.sri.com>
Thu, 6 Mar 2003 07:43:42 -0800

Visa International (with over 1 billion credit cards in circulation) is introducing a new company policy today prohibiting the display of all but the last four digits of a credit-card number on consumer receipts, a move intended to better protect customers' privacy and reduce identity theft. The policy will also remove the expiration date from receipts. The newly proposed Senate Identity Theft Protection Act would make this policy

mandatory for all credit-card companies. (Since 2000, identity theft has consistently been the most common complaint to the Federal Trade Commission, with over 160,000 complaints in 2002.) [Source: Chris Baker, *The Washington Times*, 6 Mar 2003; PGN-ed]
<http://washingtontimes.com/business/20030306-3647521.htm>

✶ Credit-card fraud

"Thomas Kristmar" <TK@dip.dk>
Wed, 05 Mar 2003 12:11:38 +0100

An interesting story in a Danish newspaper (in danish, alas)
<http://www.bt.dk/Forside.pl?aid=130204>

A postman intercepted the new credit card sent to a bank client and waited a few days and then intercepted the pincode also. The postman made a copy of the credit card and read the pincode before delivering the card and pincode a few days later to the client. Then he waited a few months. The postman was caught because he used the card excessively in a 14-day period, stealing the equivalent of 24.000 euro. [That's 24,000 euro in English. PGN]

The problem here is that all Danish credit cards and pincodes are issued from one location in plain envelopes with a return address. A postman can easily identify the cards and pincode letters. The pincode is printed in a tamperproof envelope, but affixing a "sorry, the envelope was damaged during

handling" from the Postoffice will fool the average customer.

✦ Credit company's customer list leaked to an underground gang

Chiaki Ishikawa <ishikawa@yk.rim.or.jp>

Wed, 05 Mar 2003 21:04:52 +0900

On Japanese TV nightly news, I just learned that a large Japanese credit corporation, called Orient Corporation, fired a local branch manager-level senior employee who had leaked the list of about 15,000 customers with credit card usage, etc. to a member of a Japanese gang syndicate, who in turn blackmailed the company and demanded 200,000,000 YEN. Both were arrested by police today.

Computers have made it so easy to steal such large list of customer information (to wit, involving 8 million credit-card users in the past couple of weeks). If such weakness is employed by an insider, then it would be really difficult to protect such information at all.

In this case, it was a senior employee, who was second in command to the local branch manager, and so my hope of protecting such information from abuse is now getting very thin.

Orient Corporation web page (in Japanese)

<http://www.orico.co.jp/orico/index.asp>

PS: At least, this company is quick to publicize the response to this

incidence: the web page has a link to this blackmailing incident. Oh, wait, the link failed to show the contents yet. Since the arrest was announced only a couple of hours ago, maybe the web site is going through change at 21:00. I saw the TV news only about 10 minutes ago.

★ 16M Yen stolen from sniffed bank passwords at Internet Cafe

Chiaki Ishikawa <ishikawa@yk.rim.or.jp>

Fri, 07 Mar 2003 00:40:28 +0900

On March 6th, two men have been arrested for illegally transferring 16 million YEN from someone's CityBank online banking service account to a third party account and then take the money from it, Tokyo police announced.

From the descriptions of newspaper articles, it seems that one of the culprits has installed keyboard sniffer programs on about hundred PCs at a dozen or so Internet Cafes in Tokyo and Kanagawa prefecture (south of Tokyo). He has regularly visited the cafes and brought back the recorded data with him, and searched for ID/password, and other identification information.

At the charged man's home, the police has found ID/password for 719 accounts, and about a couple of hundred user profiles meant for dating services.

One such ID/password for a man's City Bank online banking

service was used
to transfer 16 million Yen to a different account at another
bank from which
the money was withdrawn.

This is the first time that a keyboard sniffer is implicated in
a large
scale ID theft in Japan, from what I know.

It beats me, though, why anyone wants to use a PC at Internet
cafe for one's
banking service. (We should assume doing something on it, like
writing a
memo, for example, is akin to writing on a memo pad on a desk at
a public
library under which a carbon paper may be secretly placed to
record
information and we never know. For that matter, even without the
carbon
paper, we often can see the telephone number, etc. left by the
previous user
by looking at the indented marks on the next paper sheet, don't
we?)

I think the general public should be taught more about the
security
implications of various Internet services, which may look useful
and handy
on the surface, but may not be so attractive if the security
implications
are taken into account. I think it should be the responsibility
for the
service provider to tell such risks, but I am not sure how to go
about
writing a law because "risk" is a relative thing.

This has been a busy week for computer security professionals in
Japan.

First the computer system for handling nations's flight plans
collapsed on
the morning March 1st. Then a large credit card company,
Oriental Corp.,
announced the leak of 15,000 user profiles to a member of an

underground
gang group who blackmailed the company and was arrested. Then
this
incident.

I hope the general public will start to pay more attention to
the computer
security issues thanks to these high-profile incident. (The ID
theft using
keyboard sniffer was the front page head line article in the
evening edition
of *Asahi Shimbun*. It occupies about 1/5 of the paper and is
very
conspicuous.)

✶ Wrongly jailed woman blames system

"Fuzzy Gorilla" <fuzzygorilla@euroseek.com>

Tue, 04 Mar 2003 19:21:38 -0500

Excerpts, FG-highlights and PGN-ed summarization of a long item
from 11Alive News, Jennifer Leslie, 30 Jan, 10 Feb, 24 Feb 2003:

http://www.11alive.com/news/news_article.asp?storyid=27020

http://www.11alive.com/news/news_article.asp?storyid=28128

"In the first part of this report, 11Alive News Investigative
Reporter

Jennifer Leslie focused on problems with some information in
the National

Criminal Information Computer System that led to as many as 25
percent of

all arrest warrants in Metro Atlanta being inaccurate and
incomplete or

invalid. In the second part, Leslie's report focuses on what
happens when

police officers arrest the wrong person because of problems in
the

system."

Highlights (FG):

- * As many as 25 percent of all arrest warrants in Metro Atlanta are inaccurate, and incomplete or invalid. This average is eight times the national average.
- * It is easy to confuse two people that share part of a name in common.
- * It is easy to have cascading errors -- once the name was wrong, someone else added a wrong SSN.
- * Guilty until proven innocent -- if you lose your receipt, you can spend a long time trying to correct a mistake.
- * It is hard to justify success/failure rates if no records are kept.

Mistaken identity (PGN-ed):

- * Melissa Long (8.5 months pregnant) and her husband were stopped by police for a missing license plate. After an NCIC check, she was handcuffed and jailed for 10 hours in a 6x8 cell with five other women, supposedly for an outstanding warrant for domestic violence. It was eventually realized that the warrant was for someone else with the same name, but different middle names and birth dates. The Sheriff's office had added to the confusion by putting the wrong SSN on the NCIC warrant and leaving other information unspecified. Because she was already in the county computer as a witness in an unrelated case, the police used THAT info to fill out her arrest warrant!

Expired warrants (PGN-ed):

- * Innocent people across Metro Atlanta are going to jail because their old arrest warrants were never taken out of a statewide computer system.

* Nicole Thomas needed a criminal background check to apply for a job as

a teacher at her son's daycare center in August 2001, As a result, she

was jailed -- because of a warrant for an expired tag. But that warrant

should have been withdrawn because she had already paid the fine. (She

was not allowed the customary phone call.)

* One other similar case discussed in detail.

* Procedures to prevent this kind of abuse are not followed.

Error rates for the 11 metro departments:

Atlanta Police Dept.

2001 18%

1999 1.8%

Cherokee County Sheriff's Dept.

2002 16%

2000 22%

Clayton County Sheriff's Dept.

2001 21.6%

1998 16%

Cobb County Sheriff's Dept.

2001 22%

1998 22%

Dekalb County Sheriff's Dept.

2000 57%

1998 40%

Douglas County Sheriff's Dept.

2001 7%

2000 22%

Fayette County Sheriff's Dept.

2000 0%

2002 0%

Fulton County Sheriff's Dept.

2000 80% (more recent audit shows 5%)
1998 28%

Gwinnett County Sheriff's Dept.
2001 28% (more recent audit shows 6.6%)
1999 31%

Henry County Sheriff's Dept.
2002 20%
2000 30%

Smyrna Police Dept.
2001 16%
1998 16%

⚡ Re: Reversed 2002 election results in Alabama still unexplained

"Dale Pennington" <Dale.Pennington@tbe.com>

Tue, 4 Mar 2003 08:49:41 -0600

(PGN-ed, [RISKS-22.60](#))

I wish you had read the article a little more carefully. As I live in Alabama I followed this story carefully.

The time line is that on election night the unofficial total posted to the press by the county showed Don Siegelman(D) as winning. This was considered suspicious as the county is question tends to vote heavy Republican. It was determined that while the precinct totals were correct, the overall total (which was not official) was wrong by 6300 votes in Siegelman's favor. When corrected, Bob Riley(R) was the winner of the county and the state.

The Mobile Register article is consistent with the above. It says the cartridge that was used to get the first night total (Siegelman wins) was in error and the ballot count backed up the eventual (Riley) winner. The question is how the cartridge used to get the unofficial totals the first night went bad.

To sum it up, the person who got the most votes DID win.

✶ Re: Reversed 2002 election results in Alabama still unexplained

"Peter G. Neumann" <neumann@csl.sri.com>

Wed, 5 Mar 2003 8:58:30 PST

(Pennington, [RISKS-22.61](#))

Many thanks to Dale. I'm glad to be able to correct the RISKS record.

I reread the original article repeatedly, and I can see why I reached a misinterpretation in my conclusions. The article was ambiguous as to how the final official count was reached. In this case, the overall process is complicated, with integrity and reliability risks throughout -- relating to the optical-scan ballots, the local tabulation device that scans them, the cartridge that records the local results, the paper record of the local results, the aggregate centralized counting process, and the resolution of any conflicts.

Here are two of the relevant paragraphs from the cited article.

Initial, unofficial results from Baldwin County showed that Democrat Don

Siegelman garnered about 19,070 votes in the county, enough to give him a

razor-thin victory over Republican challenger Bob Riley. The next

morning, however, officials said those totals were inaccurate and

certified returns giving Siegelman about 6,300 fewer votes -- enough to

swing the election to Riley.

[...]

Officials have traced the problem to a data pack from the Magnolia Springs

voting location. They said the vote-counting machine there printed out

accurate results when the polls closed at 7 p.m. But they said the

cartridge, which resembles an eight-track cassette, gave bogus figures

when it was plugged into the computer in Bay Minette.

An important conclusion from this case remains. In the absence of an actual

recount of the hardcopy ballots (which is especially a problem with

all-electronic voting systems in which there is no voter-verified paper

record), there remain questions as to whether there was fraud or error. In

this case, the detected discrepancy among the paper counts, the cartridges,

and the final total forced a reassessment (but not a recount).

But in cases

of disagreement, it is important to be able to ascertain what is correct.

The deeper implication of this case is of course that in the absence of

meaningful audit trails and voter-verified ballots or ballot

images, the entire election process can be subject to unresolvable questions. In all-electronic systems, the absence of a voter-verified ballot image makes it possible in any voting machine for the electronic totals at the end of the day to agree completely with the printed totals, but for both of them to be seriously in error, for any of a variety of reasons.

✈ **Re: Computer error grounds Japanese flights ([RISKS-22.60](#))**

Chiaki Ishikawa <ishikawa@yk.rim.or.jp>

Wed, 05 Mar 2003 21:04:52 +0900

The Ministry Web page finally had a short comment about the incident (in Japanese, of course) on 3 Mar, whereas the incident occurred on 1 Mar. I know it was a weekend, but since I noticed a well-attended press conference about the incident over TV, I would think a brief transcript of the presentation would have been enough and useful to put on the Web to the many Japanese who tried to learn what was going on on Saturday.

The following is the short notice, mostly the expression of the apology, not much detail about the technical problem which I learned from newspaper articles.

<http://www.mlit.go.jp/koku/030301.html>

⚡ Re: BSA Accuses OpenOffice ftp sites of piracy ([RISKS-22.60](#))

Fritz Whittington <f.whittington@att.net>

Tue, 04 Mar 2003 17:19:57 GMT

Since they state "the information in this notification is accurate and states, under penalty of perjury, that it is authorized to act in this matter" then, considering that the information is patently false, to which jurisdiction do we report their perjury? The EU courts, the US courts? Perhaps both? Is it possible to commit perjury when you aren't testifying?

Sigh. The computer-related risk here is enormous. Dependence on computers is apparently making a significant fraction of the population incurably stupid.

⚡ New IEEE Security and Privacy magazine

Gary McGraw <gem@cigital.com>

Thu, 6 Mar 2003 08:56:22 -0500

The IEEE Computer Society has created a new magazine called "Security and Privacy" specifically for the security community <<http://www.computer.org/security/>>. The magazine intends to present a balanced mix of scientific research and practical security discussion. One key aim is to cut through the security hype promulgated by commercial trade magazines. The first issue came out last month. The editorial

board is
eager to publish cutting edge research in the peer-reviewed
section of the
magazine. Send your best papers to <sprivacy@computer.org>.
Also as a
member of the task force, I welcome candid feedback via e-mail.

✦ REVIEW: "Security in Computing", Charles Pfleeger/Shari Pfleeger

Rob Slade <rslade@sprint.ca>
Wed, 5 Mar 2003 08:01:41 -0800

BKSCNCMP.RVW 20030209

"Security in Computing", Charles P. Pfleeger/Shari Lawrence
Pfleeger,

2003, 0-13-035548-8, U\$79.00/C\$122.99

%A Charles P. Pfleeger

%A Shari Lawrence Pfleeger s.pfleeger@ieee.org

%C One Lake St., Upper Saddle River, NJ 07458

%D 2003

%G 0-13-035548-8

%I Prentice Hall

%O U\$79.00/C\$122.99 +1-201-236-7139 fax: +1-201-236-7131

%O <http://www.amazon.com/exec/obidos/ASIN/0130355488/>

robsladesinterne

<http://www.amazon.co.uk/exec/obidos/ASIN/0130355488/>

robsladesinte-21

%O <http://www.amazon.ca/exec/obidos/ASIN/0130355488/>

robsladesin03-20

%P 746 p.

%T "Security in Computing"

This work is still obviously a textbook. The attempts to target
it at a
"professional" audience are possibly more convincing than in the
first

edition, but it still reads like a text, and includes material that is addressed at a scholastic, rather than experienced, audience. Even as a textbook it difficult to say that it succeeds. It addresses a broad range of computer security related topics, although there is a notable shortage of material dealing with formal security models, access concepts, operational procedures, physical security, and business continuity. The level of detail in the different areas varies greatly, but the shortcomings of the book could be addressed in the hands of a competent teacher.

The ten chapters in the book are not divided into parts, but seem, in some cases, to come in chunks. The introductory chapter is an overview of basic concepts involved with system security. Unfortunately, not all of them are explained fully. The idea of controls, for example, is a vital one, but the full ranges and types of controls are not outlined. There are also some not-quite-standard additions to the lexicon, such as an attempt to divide threats into four classes: interception, interruption, modification, and fabrication. It is difficult to see why fabrication is added to the list, or why this provides a clearer view of threats than simply looking to the opposites of confidentiality, integrity, and availability. Cryptography starts in chapter two (and, oddly, ends in chapter ten). The early coverage steps through different types of simple encryption algorithms, followed up by cryptanalysis of the same. It strenuously avoids using any arithmetic, which makes discussions of key sizes and strengths a bit

difficult, but
throws in lots of symbolic logic, which seems to serve only to
cloud the
issue.

Chapter three starts what might be seen as a section on secure
systems
development. This is an important, and often neglected, topic,
and is
generally covered reasonably well. However, the material is not
always
completely clear and rigorous. For example, it is implied that
Thompson,
rather than Cohen, was the first to investigate viruses.
Leaving aside the
fact that Cohen's work started a year before Thompson's lecture
(only the
date of Cohen's graduation is given), Thompson's thought
experiment proposed
only an extremely limited form of reproduction. Again, when
discussing
covert channels, both the terms "timing channel" and "storage
channel" are
used, but all the examples given relate only to timing
channels. Operating
system protections are supposed to be covered in chapter four,
but the
content is an odd amalgam of computer architecture and high
level access
control. In regard to designing trusted operating systems,
chapter five
starts with a very poor outline of formal models (the test is
not clear,
and, again, the addition of symbolic logic fails to assist in
the tutorial),
presents a fair review of operating system requirements, and
then spends a
lot of time going over various evaluation criteria, without
presenting much
content of any use. The outline of database security is
disappointing:
chapter six spends too much time on specific details, while
almost ignoring

major concepts such as aggregation.

Chapter seven, the longest in the book, devotes excessive space to basic communications technologies, including two copies of the section on transmission methods. Administration, in chapter eight, provides the usual generic advice on planning, risk, and policies. Intellectual property, computer crime, and ethics are presented as problems with no solutions, in chapter nine. The closing chapter provides a whirlwind of the mathematics related to cryptography in an impressive, disorganized, and basically pointless display.

This book could definitely use a wholesale reorganization and cleanup. The level and tone of the content varies tremendously from section to section, even within given chapters. While most computer security topics appear somewhere within the work, there is very little in the way of logical flow or links between subjects. Major areas seem to be thrown in with minor sections simply because they had to be put somewhere. In terms of textbooks, I do not know that there is much to choose between this volume and Bishop's "Computer Security: Art and Science" (cf. BKCMSCAS.RVW), although Pfleeger and Pfleeger might have a slight edge. Certainly Gollman's "Computer Security" (cf. BKCOMPSC.RVW) is superior to both. And, depending upon the course, Anderson's "Security Engineering" (cf. BKSECENG.RVW) probably outranks them all.

copyright Robert M. Slade, 1993, 2003 BKSCNCMP.RVW 20030209
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca

p1@canada.com

[http://victoria.tc.ca/techrev
~rslade](http://victoria.tc.ca/techrev/~rslade)

or

<http://sun.soci.niu.edu/>



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 62

Monday 10 March 2003

Contents

- [Identity mixup: NZ teacher identified as prostitute](#)
[Ruth Berry via Max Power](#)
- [The darkest side of ID theft](#)
[Bob Sullivan via Monty Solomon](#)
- [Wrong man arrested after identity theft](#)
[Neil Youngman](#)
- [Microsoft speaks, site goes dark](#)
[Joe Wilcox via Monty Solomon](#)
- [Computer crashes threaten hospital operations](#)
[Monty Solomon](#)
- [Toronto public health computer accidentally erases records](#)
[Chris Smith](#)
- [Inappropriate HMI on medical device](#)
[Erling Kristiansen](#)
- [Security firm shuttered by sabotage](#)
[Andrew Colley via Keith Rhodes](#)
- [Sendmail flaw tests Homeland Security](#)
[Robert Lemos via Monty Solomon](#)
- [Hackers access University of Texas database](#)
[Mike Swaim](#)
- [You might just be a hacker if...](#)
[Andrew Orłowski via Tim Finin](#)
- [Kevin Poulsen: Windows root kits a stealthy threat](#)
[Monty Solomon](#)
- [FirstUSA/BankOne sends login ID & PW as clear text](#)

[Ric Cohen](#)

- [Nigerian scams continue to thrive](#)

[Monty Solomon](#)

- [Traffic lights don't work in the snow](#)

[Bob Copeland](#)

- [Re: Computer error means 2.3-trillion-pound electricity bill](#)

[Michael Bacon](#)

- [Re: Someone protecting patient data well](#)

[Edwin Culver](#)

- [Re: BSA Accuses OpenOffice ftp sites of piracy](#)

[Fuzzy Gorilla](#)

- [Re: Visa moves to improve customers' privacy](#)

[Brett Glass](#)

[Margie Wylie](#)

- [New article on critical infrastructure risks](#)

[Fred Cohen](#)

- [Info on RISKS \(comp.risks\)](#)

⚡ Identity mixup: NZ teacher identified as prostitute

Max Power <mikehack@u.washington.edu>

Thu, 6 Mar 2003 18:14:45 -0800 (PST)

Michelle Garforth (Dunedin, NZ) applied to be registered as a teacher, after finishing four years of training. She was notified that she was "likely" to be a prostitute convicted on four charges, including two assaults, based on a computer match of her maiden name and birthdate. Despite going to the police and submitting to fingerprinting that demonstrated she was not the person in question, she was not cleared until weeks later -- after her local Member of Parliament had intervened. [Source: Prostitute mix-up shocks teacher, by Ruth Berry, 06 March 2003; PGN-ed]

<http://www.stuff.co.nz/stuff/0,2106,2309649a7694,00.html>

⚡ The darkest side of ID theft

Monty Solomon <monty@roscom.com>

Mon, 10 Mar 2003 09:49:24 -0500

Malcolm Byrd was confronted at home by three Rock County, Wisconsin, sheriff's officers with a warrant for Byrd's arrest for cocaine possession, with intent to distribute. He tried to tell them that he was a victim of identity theft. So, he was handcuffed and taken away. Again!

"This is the worst-case scenario for identity theft victims. Losing your clean credit history is one thing; losing your freedom is another. And victims of America's fastest-growing crime are discovering they often have much more to worry about than the hundreds of hours of paperwork necessary to clean up the financial mess associated with ID theft. Sometimes, they have to worry about ending up in jail - again and again." [Source: ...

When

impostors are arrested, victims get criminal records, Bob Sullivan, MSNBC, 9

Mar 2003; PGN-ed]

<http://www.msnbc.com/news/877978.asp>

✦ Wrong man arrested after identity theft

Neil Youngman <n.youngman@ntlworld.com>

Sun, 9 Mar 2003 19:55:25 +0000

A British man was arrested in South Africa and held for 2 weeks on an FBI warrant after his identity was stolen by a fraudster. He was only released after the real suspect was picked up in the U.S.

<http://news.bbc.co.uk/1/hi/england/2806827.stm>

✦ Microsoft speaks, site goes dark

Monty Solomon <monty@roscom.com>

Sat, 8 Mar 2003 17:28:46 -0500

Microsoft speaks, site goes dark, by Joe Wilcox, CNET News.com, 7 Mar 2003

In an uncommonly harsh application of a widely used Internet enforcement tool, a Windows news site was taken offline for nearly 24 hours this week after Microsoft accused the site of infringing its copyrights.

Neowin was shut down late Thursday and came back online Friday afternoon.

Microsoft's Internet investigator sent a takedown notice on Tuesday, alleging the site was infringing the company's copyrights relating to its recently released Windows XP Peer-to-Peer Software Development Kit (SDK), apparently due to a message posted by a reader in an online feedback forum.

Such legal filings are routine. But in this case, the request turned into a nightmare for Neowin when it was sent not to the site but to the upstream Internet service provider responsible for Neowin's Web connection. That provider responded by pulling the entire site offline. Neowin declined to name the ISP, but a traceroute on the Neowin.net address showed Williams Communications Group, now known as WillTel Communications, as its furthest upstream provider. Sources later confirmed that Microsoft contacted the closer upstream provider, Hurricane Electric Internet Services of Fremont, Calif.

Neowin and its Web host, Invision Power Services Hosting (IPS), blamed Microsoft for the incident, saying the software giant gave them no chance to fix the problem before referring it to the ISP for more draconian measures.

[...]

<http://news.com.com/2100-1025-991624.html>

⚡ Computer crashes threaten hospital operations

Monty Solomon <monty@roscom.com>

Sun, 9 Mar 2003 00:28:12 -0500

Beth Israel Deaconess Medical Center was paralyzed for four days by a computer crash in November 2002. Dr. Peter Kilbridge, an independent consultant who reviewed the incident at Beth Israel at the request of the *New England Journal of Medicine* editor, Dr. Jeffrey Drazen, said even if hospitals have policies in place to encourage the appropriate use of computers, those policies are often are ignored. [Source: Associated

Press,

7 Mar 2003]

[http://www.boston.com/dailynews/066/
region/Computer_crashes_threaten_hosp:.shtml](http://www.boston.com/dailynews/066/region/Computer_crashes_threaten_hosp:.shtml)

✦ Toronto public health computer accidentally erases records

Chris Smith <smith@interlog.com>

Mon, 10 Mar 2003 08:52:26 -0500 (Eastern Standard Time)

As reported 10 Mar 2003 *Toronto Star*, GTA section, page B5:

"Health records feared erased"

A computer fault may have accidentally erased the immunization records of

thousands of Toronto school children, the city's public health department

fears. Last April, the department discovered that its immunization records information system was erasing files from among 425,000 student records, Dr. Barbara Yaffe, associate medical officer of health, said. "It appears it was randomly erasing files - and we don't know how many," Yaffe said.

The department tried to get technical help from the provincial health ministry, but its technicians were among the 45,000 Ontario civil servants

taking part in a 54-day strike last spring.

I suppose this is better than the traditional health info problem of accidental privacy breaches, but not by much. The department will have to contact parents to have them supply -- again -- the immunization status of their children in the above cases.

This is especially important since failure to ensure appropriate immunizations can possibly result in suspension of children from school.

Article is online at...

[http://thestar.ca/NASApp/cs/ContentServer?pagename=thestar/Layout/
Article_PrintFriendly&c=Article&cid=1035778928098&call_pageid=968350130169](http://thestar.ca/NASApp/cs/ContentServer?pagename=thestar/Layout/Article_PrintFriendly&c=Article&cid=1035778928098&call_pageid=968350130169)

⚡ Inappropriate HMI on medical device

Erling Kristiansen <erling.kristiansen@xs4all.nl>

Sat, 08 Mar 2003 20:38:46 +0100

I spent some time in a hospital recently. The patient next to me, a woman in her late seventies, was being treated with a suction pump to remove fluid from an infected operation wound.

This pump was a very neat, portable, lightweight device that allowed the patient to move around relatively freely. After a few days, the patient was sent home. A short instruction course was given to her and her husband, who was about the same age.

The next day, she was back. In tears and very depressed. Her husband did not accompany her: He had had a nervous breakdown.

They had been unable to figure out how to operate the pump.

I did not want to interfere directly, but tried to figure out from conversations, events and casual inspection what the HMI of the pump looked like. It was a menu-driven interface with a small LCD display and at least 4 push-keys. Activating the pump seemed to require at least 4 key-pushes, as did resetting the alarm that went off if the device was not operating properly for more than a given time. As far as i could figure out, some of the 4 steps were actually going through menus that allowed to re-configure the operating parameters, so a real risk existed of accidentally changing the setup.

A scenario that played out several times, was: The patient wanted to go to the bathroom at night; she disconnected mains power (switching from mains to battery and back seemed to require operator intervention); after some 15 menus, the alarm went off; pushing any key seemed to reset the alarm, that then went off again 15 minutes later. And so on. The poor lady was so embarrassed keeping other patients awake that she even tried to wrap the device in towels to subdue the alarm! Most of the medical staff did not know how to operate the pump, either, so much confusion ensued, often resulting in a trial-and-error scenario.

My remarks:

- A medical device designed to be operated by patients, and in particular elderly patients, should have a very clear separation between configuration HMI and routine operation HMI. The configuration HMI should be lockable or mechanically shielded to prevent accidental operation.
- The patient HMI should be as simple as at all possible, preferably a single on/off or enable/disable switch and a very clear indication whether the device is operating.
- Alarm handling, if needed, should be simple and clear. In particular, reacting on an alarm, it should be immediately obvious whether the alarm condition had been solved or persisted. A design where the alarm is reset, just to re-appear after a time-out, because the underlying cause was not resolved, is confusing.
- Switching between mains and battery power should be fully transparent to the user.

⚡ Security firm shuttered by sabotage

Keith Rhodes <rhodesk@gao.gov>
Tue, 4 Mar 2003 04:09:21 -0800 (PST)

The enemy could be sitting next to you. An Australian security firm was forced to close due to a major internal security breach -- reportedly caused by a disgruntled employee. [Andrew Colley, ZDNet Australia, 3 Mar 2003]
<http://zdnet.com.com/2100-1105-990747.html>

⚡ Sendmail flaw tests Homeland Security

Monty Solomon <monty@roscom.com>
Wed, 5 Mar 2003 16:19:31 -0500

A critical flaw in Sendmail, the Internet's most popular e-mail server, has become the first test for the newly minted Department of Homeland Security

and its cyberdefense arm. The agency's Directorate of Information Analysis and Infrastructure Protection (IAIP) worked with security company Internet Security Systems, which discovered the flaw, and Sendmail Inc. to create a patch while keeping news of the issue from leaking to those who might exploit the vulnerability. "Working with the private sector, we alerted key owners of the vulnerable software and got them talking," said David Wray, spokesman for the IAIP Directorate. "We think this is a great example of how this should, and does, work."

Word of the vulnerability, which would let an attacker take control of a Sendmail server and execute a malicious program, was more widely disseminated Monday. The Department of Homeland Security got high marks from the security community for giving companies the necessary time to create the patch and for synchronizing its release. [...]

Robert Lemos, CNET News.com, 3 Mar 2003
<http://news.com.com/2100-1009-990879.html>

🔥 Hackers access University of Texas database

Mike Swaim <swaim@hal-pc.org>
Thu, 06 Mar 2003 21:09:04 -0600

According to the **Houston Chronicle**, hackers were able to obtain information, including Social Security numbers on 59,000 former and current students, staff and faculty members between 26 Feb and 1 Mar 2003. "The theft was discovered Sunday evening by university computer systems employees performing routine maintenance, Updegrave said. They immediately disconnected the compromised database from the Internet, later hooking up a database of useless information. Computer logs indicate the information was taken by a computer in Austin on Wednesday, Thursday and Friday last week and by a computer in Houston on Saturday and Sunday, Updegrave said. He said the intrusions were likely done by the same person or persons, he added." The obvious risk is having a production system directly accessible from the Internet.

<http://www.chron.com/cs/CDA/ssistory.mpl/front/1806724>

[Also noted by David Newman from the *Austin American-Statesman*:

<http://www.austin360.com/aas/metro/030603/0306uthack.html>

http://www.austin360.com/aas/metro/030603/0306uthack_update.html

citing 55,200 SSN/Name pairs; David added

"I admire the willingness of the VP to admit to a failure in his department. His honesty is refreshing in the Age of the Lawyers."

Also noted by Fuzzy Gorilla from the same news account, from slashdot:

<http://slashdot.org/articles/03/03/06/1720224.shtml>

which again used the 59,000 number. PGN]

⚡ You might just be a hacker if...

Tim Finin <finin@cs.umbc.edu>

Mon, 10 Mar 2003 01:30:25 -0500

... you vote the wrong way in Senate Majority Frist's poll. That 60% of the Internet voters were against a pre-emptive invasion of Iraq doesn't seem like evidence of hacking. Frist's site claimed that only one vote per person was counted. I assume they had implemented a trivial "One IP address, one vote" check, which, while subject to subversion, was probably more ok than not.

Senate Leader scraps Web site war poll, blaming hackers
Andrew Orlowski, 7 Mar 2003

<http://www.theregister.co.uk/content/55/29654.html>

Senate majority leader Bill Frist has yanked a "Bomb Iraq" poll from his Web site.

Frist's office told The Register that "tampering" was to blame for the removal of the poll, which asked "Should the United States use force to remove Saddam Hussein from power? Your opinion is important to Senator Frist."

"Clever computer programmers created a program that generated 8,700 votes in a day," a spokesperson told us. Which is where the mystery really begins.

The spokesperson couldn't say whether the software was running inside the firewall, representing a major breach of the Senate IT security, or was a robot-style vote generator run by netizens.

The curious thing is that Frist's poll page already banned robots - including the Wayback Machine, archive.org - from the site. Respondents could vote once and then return to the site later to change their vote; only the latest response would be counted.

"As you know government computers are constantly being attacked by hackers," he suggested.

Nor could Frist's office explain why the Web site administrators simply didn't exclude the votes they didn't want to count - Florida-style.

One correspondent has noted the increasing tally of No votes:-

"At 1:35 pm Washington DC time on March 6, the Frist site reported 31,118 responses to the war poll. Anti-war respondents (55%) had gained a clear majority over pro-war respondents (44.6%). (These figures do not quite add up to 100%, apparently because of the rounding method used by Senator Frist's staff.)

"Within the hour, at 2:23 pm, the anti-war fever had risen, with 56.9% anti-war, 42.9% pro-war. By 4:29 pm, according a snapshot of the Frist site, with 37, 742 total responses, the anti-war vote registered 59.5%, with the pro-war vote ebbing at 39.8%."

The Senate site has been defaced before. Whether this represents a new and more serious breach - as Frist's office suggests - we don't know.

But our enquiries continue.

⚡ Kevin Poulsen: Windows root kits a stealthy threat

Monty Solomon <monty@roscom.com>

Mon, 10 Mar 2003 09:16:00 -0500

Hackers are using vastly more sophisticated techniques to secretly control the machines they've cracked, and experts say it's just the beginning.

By Kevin Poulsen, SecurityFocus Mar 5 2003 5:12AM

Barron Mertens admits to being puzzled last January when a cluster of

Windows 2000 servers he runs at an Ontario university began crashing at random. The only clue to the cause was an identical epitaph carved into each

Blue Screen of Death, a message pointing the blame at a system component called "ierk8243.sys." He hadn't heard of it, and when he contacted Microsoft, he found they hadn't either. "We were pretty baffled," Mertens recalls. "I don't think that cluster had bluescreened since it was put into

production two years ago."

Mertens didn't know it at the time, but the university network had been compromised, and the mysterious crashes were actually a lucky break -- they

gave away the presence of an until-then unknown tool that can render an intruder nearly undetectable on a hacked system. Now dubbed "Slanret", "IERK," and "Backdoor-ALI" by anti-virus vendors, experts say the tool is a

rare example of a Windows "root kit" -- an assembly of programs that subverts the Windows operating system at the lowest levels, and, once in place, cannot be detected by conventional means. [...]

<http://www.securityfocus.com/news/2879>

⚡ FirstUSA/BankOne sends login ID & PW as clear text

Ric Cohen <cohen@aros.net>

Thu, 6 Mar 2003 22:20:08 -0700

This afternoon, I attempted to review my credit card account by logging in at: <http://cardmemberservices.firstusa.com/index.jsp> as I have for several years. My security software stopped the login and warned me that the Web page was attempting to send my password as clear text. I phoned the number on the Web page to report this, and eventually got to a low level tech. After he said that no one in the company had changed the Web page software for a long time, I pointed out this implied the Web site was hacked. He said he would report the problem. After an hour, I concluded that this person didn't appreciate the fact that a hacker reading the login

information would also have access to credit card numbers. I attempted to access the same Web site, and was redirected to:

<http://online.firstusa.com/bolHOME.aspx>

-- which presented a Web page identical to that on the first Web site.

The

same problem appeared when I attempted to login.

The problem centers upon a risk I have wondered about for years. None of BankOne's (or its' subsidiaries) login Web pages begin on a secure https page. They require you to enter your user ID and password on an insecure http page, and this information is supposed to be encrypted immediately prior to submission. They even have a friendly 'security help' page which describes how this *should* work without problem. I never trusted this approach which is used on several Web sites, and that is why I use software which monitors for passwords.

Because my software always stopped the login process as the password was about to be sent, I decided to experiment. I chose a nonsense login ID and password, and set my software to look for them both (but allow them to be sent to FirstUSA). What I observed was both the ID and password text being sent several times by TCP port 80, to the bank's IP 159.53.21.247. Only then, did the Web page change to a secure page using port 443, and tell me that it did not know me.

After this happened, I called a local bank branch just before closing time, described the problem, and got a phone number for the 'Office of the Chairman'. I talked with someone who seemed intelligent, who seemed to understand that credit card numbers could be stolen if someone were to make use of customer's login information, and who seemed to agree that the Web site should be shut down. However, 6 hours later, I write this as the Web site is still (dys)functioning as before.

The last time I logged into FirstUSA was Feb. 27 (without a problem). Somewhere between then and today, their Web site was altered and who knows what problems will eventually come of this. FWIW, I attempted earlier to login at <http://www.bankone.com> with my nonsense ID and PW. They were encrypted properly, and nothing at all was sent clear text. I have not tried their other subsidiary's Web sites.

[Added by Ric 7 Mar 2003:]

There is now a new Web site that requires login in a secure environment: <https://online.firstusa.com/bank/bolLogin.aspx> However, the same Web site mentioned in the last note (which has existed for years) still exists today and continues to transmit user login info as clear text.

⚡ Nigerian scams continue to thrive

Monty Solomon <monty@roscom.com>

Sun, 9 Mar 2003 14:56:37 -0500

Cashier's checks, Iraqi plea add two new flavors to old story

By Bob Sullivan, MSNBC, 5 Mar 2003

Two new flavors of the age-old Nigerian e-mail scam are making the rounds, and at least one of them appears to be gaining traction. Hundreds of victims

have recently fallen for a variation that plays upon people's misunderstanding about how bank cashier's checks work. Meanwhile, other scammers are trying to take advantage of heightened interest in Iraq, posing

as frightened Iraqis trying to move money out of that country before hostilities begin. The scam also took a deadly turn last month, when a victim in the Czech Republic allegedly shot and killed a Nigerian diplomat after losing his life savings to the scam. [...]

<http://www.msnbc.com/news/881169.asp>

⚡ Traffic lights don't work in the snow

Bob Copeland <bobc@ieee.org>

Mon, 3 Mar 2003 21:43:03 -0500

In my area, northern Virginia, nearly every intersection is outfitted with inductance loops -- sensors for detecting when a large metal object (often, a car) sidles up to a traffic light. Ideally, this is so it turns green more quickly for you, but of course in practice, it usually turns green more quickly for the other guy. Most of these intersections operate in normal turn-based fashion but speed up or slow down when cars are present.

However, at least one such light refuses to turn green unless there is a car present. Recently, a 24 inch snowfall and a snow plow conspired to bury the sensor at that light under a mountain of ice, so when I approached it last weekend, the car ahead of me and I had to stop in the left turn lane. After sitting at red for 2 cycles, we gave up and ran it. One more risk of driving in the snow!

⚡ Re: Computer error means 2.3-trillion-pound electricity bill

<michael_bacon@synigystic.com>

Sat, 8 Mar 2003 05:40:15 -0000

([RISKS-22.61](#))

Two things in particular surprise me about this. The first is that apparently someone designed a system that would accommodate a consumer bill reaching into the trillions of pounds. The second is that there were seemingly no validity (or common sense if the letter was hand-typed) checks that detected a consumer bill many times the UK National Debt!

Of course this could be the same sort of "clerical error" that led Civil Servants recently to claim that they had frozen a 'Bin Laden' bank account containing 23.19 million pounds. The true figure was just 23 pounds and 19 pence!

⚡ Re: Someone protecting patient data well ([RISKS-22.60](#))

Edwin Culver <emculver@snet.net>

Fri, 07 Mar 2003 13:27:27 -0500

In a similar story to Dr O'Keefe's:

When I was working in the aerospace industry, the method we had chosen for making sure magnetic media no longer contained classified data was very simple: remove the platters from the disk drives (or the floppies from their sleeves or the tape from its reel) and sand blast the magnetic coating off. We all thought this was a mite drastic, as a degausser should scramble all the bits.

Sandblasting may be more subtle than the sysadmin at his university's medical research group, but probably quite as effective.

The mistake trying to recover the residual value of the disk drives.

⚡ Re: BSA Accuses OpenOffice ftp sites of piracy ([RISKS-22.61](#))

"Fuzzy Gorilla" <fuzzygorilla@euroseek.com>

Thu, 06 Mar 2003 17:19:41 -0500

Unfortunately, they are not claiming, under penalty of perjury, that the notification is accurate, only that they are authorized to "act in this matter on behalf of the copyright owners listed above. [Microsoft]"

Basically, they cannot legally act on behalf of someone who has not given them that authority.

⚡ Re: Visa moves to improve customers' privacy ([RISKS-22.61](#))

Brett Glass <brett@lariat.org>

Thu, 06 Mar 2003 13:29:44 -0700

[Blanking out part of the credit-card number and the expiration date] has already been the law in California for more than a year. It would actually cost them more not to have a uniform policy nationwide.

⚡ Re: Visa moves to improve customers' privacy ([RISKS-22.61](#))

Margie Wylie <mwylie@earthlink.net>

Thu, 06 Mar 2003 12:51:00 -0800

[...] Many businesses are already complying, but the final deadline for implementing the change is Jan. 1, 2004.

<http://www.bankrate.com/brm/news/cc/20010129a.asp>

⚡ New article on critical infrastructure risks

Fred Cohen <fc@all.net>

Thu, 6 Mar 2003 18:34:23 -0800 (PST)

Your readers may be interested in:

<http://all.net/>

=> InfoSec Baseline Studies

=> Cyber-Risks and Critical Infrastructures

Fred Cohen - <http://all.net/> fc@all.net fc@unhca.com tel/fax: 925-454-0171

Fred Cohen & Associates - University of New Haven - Security Posture



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

[ACM](#) Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 63

Wednesday 12 March 2003

Contents

- [Education and the National Strategy to Secure Cyberspace](#)
[Rob Slade](#)
- [IEEE Symposium on Security and Privacy](#)
[Lee Badger](#)

✦ Education and the National Strategy to Secure Cyberspace

Rob Slade <rslade@sprint.ca>
Tue, 11 Mar 2003 08:28:07 -0800

The second version of the National Strategy to Secure Cyberspace has been released.

One is reminded of the old joke: someone is in a balloon, and lost, asks a person on the ground where he is, and, upon being told that he is in a balloon, states that the person on the ground is an economist/academic/tech

support person/profession to be deprecated since the answer is completely true and completely useless. Much the same critique can be made about the National Strategy to Secure Cyberspace.

Given the fanfare and promotion of the strategy, it has been quite disappointing to see the final result. However, the area of education and training, while named as a priority, is particularly weak.

I have extracted the relevant portions of the strategy, and interlined commentary. For those who wish to access the full document, without my opening, it is available at:

http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf

> From the Executive Summary:

> Priority III: A National Cyberspace Security Awareness and Training Program

> Many cyber vulnerabilities exist because of a lack of cybersecurity

> awareness on the part of computer users, systems administrators,

> technology developers, procurement officials, auditors, chief information

> officers (CIOs), chief executive officers, and corporate boards. Such

> awareness-based vulnerabilities present serious risks to critical

> infrastructures regardless of whether they exist within the infrastructure

> itself. A lack of trained personnel and the absence of widely accepted,

> multi-level certification programs for cybersecurity professionals

> complicate the task of addressing cyber vulnerabilities.

This much we knew already. However, the proposed activities are

somewhat
limited:

- > The National Strategy to Secure Cyberspace identifies four major actions and
- > initiatives for awareness, education, and training:
 - > 1. Promote a comprehensive national awareness program to empower all
 - > Americans -- businesses, the general workforce, and the general population
 - > -- to secure their own parts of cyberspace;
 - > 2. Foster adequate training and education programs to support the Nation's
 - > cybersecurity needs;
 - > 3. Increase the efficiency of existing federal cybersecurity training
 - > programs; and
 - > 4. Promote private-sector support for well-coordinated, widely recognized
 - > professional cybersecurity certifications.

> THE NATIONAL STRATEGY TO SECURE CYBERSPACE 37

> PRIORITY III

- > Everyone who relies on part of cyberspace is encouraged to help secure the
 - > part of cyberspace that they can influence or control. To do that, users
 - > need to know the simple things that they can do to help to prevent
 - > intrusions, cyber attacks, or other security breaches. All users of
 - > cyberspace have some responsibility, not just for their own security, but
 - > also for the overall security and health of cyberspace.

While this statement is true, it seems to set a tone of "we can't do it

alone, so we're not going to do anything" in this document.

- > In addition to the vulnerabilities in existing information technology
- > systems, there are at least two other major barriers to users and managers
- > acting to improve cybersecurity: (1) a lack of familiarity, knowledge, and
- > understanding of the issues; and (2) an inability to find sufficient
- > numbers of adequately trained and/or appropriately certified personnel to
- > create and manage secure systems.

This blanket statement cries out for clarification. There is familiarity, knowledge and understanding--in those relatively few who have taken it upon themselves to study the issues. In regard to the inability to find sufficient numbers of trained individuals, I note that there are plenty of unemployed CISSPs out there. I would say, as I have said in regard to many supposed high tech labour shortages over the past couple of decades, that there is no shortage of skilled people, just a shortage of skilled people willing to work for nothing. To coin a phrase from Juvenal, all wish to know, but none want to pay the fee.

- > Among the components of this priority are the following:
- > . Promote a comprehensive national awareness program to empower all
- > Americans -- businesses, the general workforce, and the general
- > population -- to secure their own parts of cyberspace;

This is unlikely to happen any time soon. The first step towards such a program would be to determine a "minimum necessary" standard of security

awareness. Since we can't even agree on a minimum necessary level of security for products (or street-proofing for children, or intelligence necessary to order coffee, etc), we are unlikely to be able to draw this line with any clarity or speed.

- > . Foster adequate training and education programs to support the Nation's
- > cybersecurity needs;

This would be nice. How will it happen?

- > Increase the efficiency of existing federal cybersecurity training
- > programs; and

More money for sending people for training would probably be a good start.

- > . Promote private sector support for well-coordinated, widely recognized
- > professional cybersecurity certification.

How would this be accomplished?

- > Key to any successful national effort to enhance cybersecurity must be a
- > national effort to raise awareness (of users and managers at all levels)
- > and maintain an adequate pool of well trained and certified IT security
- > specialists. The federal government cannot by itself create or manage all
- > aspects of such an effort. It can only do so in partnership with industry,
- > other governments, and nongovernmental actors.

Once again, this seems to say that the government cannot do it all, so it will not do much at all.

In regard to maintaining a national pool of talent, I recall that I was approached four or five years ago by someone from a (then Clinton) Whitehouse office in regard to encouraging security experts to teach security courses at universities. My response was that such encouragement required there to be faculty positions for such experts to occupy, jobs for students of such courses to occupy when they graduated, and jobs for the experts to return to when they finished teaching. The jobs weren't there then, and they aren't there now.

(I recall a science fiction story of many years back where a nation had devoted itself to developing practical skills and efficient programs. At a crucial juncture, it became apparent that a poet was vital to the survival of the nation. A poet could not be found among the highly skilled, trained, and practical populace. Sometimes skills just can't be created on demand.)

> Many federal agencies must play a part in this effort, which will be led and
> coordinated by DHS. The components of this program will include the
> following federal programs (both existing programs and initiatives which
> will be considered as part of the budget decision making process) and
> activities, which we recommend to our partners.

> A. AWARENESS

> 1. Promote a Comprehensive National Awareness Program to Empower All
> Americans---Businesses, the General Workforce, and the General Population

> -- to Secure their Own Parts of Cyberspace

> In many cases solutions to cybersecurity issues exist, but the people who

> need them do not know they exist or do not know how or where to find

> them. In other cases people may not even be aware of the need to make a

> network element secure. A small business, for example, may not realize

> that the configuration of its web server uses a default password that

> allows anyone to gain control of the system. Education and outreach play

> an important role in making users and operators of cyberspace sensitive to

> security needs. These activities are an important part of the solution for

> almost all of the issues discussed in the National Strategy to Secure

> Cyberspace, from securing digital control systems in industry, to securing

> broadband Internet access at home.

> DHS, working in coordination with appropriate federal, state, and local

> entities and private sector organizations, will facilitate a comprehensive

> awareness campaign including audience-specific awareness materials,

> expansion of the StaySafeOnline campaign, and development of awards

> programs for those in industry making significant contributions to

> security. (A/R 3-1) Increasing awareness and education prepares private

> sectors, organizations, and individuals to secure their parts of

> cyberspace. Actions taken by one entity on a network can immediately and

> substantially affect one or many others. Because the insecurity of one

> participant in cyberspace can have a major impact on the

others, the
> actions they take to secure their own networks contribute to
the security
> of the whole. For example, a few subverted servers recently
enabled an
> attack on some of the Internet Domain Name System root servers
and
> threatened to disrupt service for many users. Through
improved awareness
> the Nation can stimulate actions to secure cyberspace by
creating an
> understanding at all audience levels of both cybersecurity
issues and
> solutions. DHS will lead an effort to increase cybersecurity
awareness for
> key audiences:

While I do not wish to belittle the importance or contribution
of the
StaySafeOnline program within its purview, it is far too limited
to function
even as a template for a larger security awareness campaign.

An awards program is probably going to have to be cold, hard
cash, in large
amounts, to counter current levels of apathy. Steve Ballmer's
speech from
1997 almost makes the case the Microsoft is the dominant
industry player not
in spite of the fact that it ignores security, but precisely
because it
ignores security. Security awareness cannot be promoted by
establishing
contests where nobody will compete.

> a. Home Users and Small Business

> Home users and small business are not part of the critical
> infrastructures. However, their systems are being
increasingly subverted
> by malicious actors to attack critical systems. Therefore,
increasing the
> awareness about cybersecurity among these users contributes to

greater

> infrastructure security. Home users and small business owners
of cyber
> systems often start with the greatest knowledge gap about
cybersecurity.

Coming from the virus research community as I do, I would say
that the first
statement here is flatly wrong. Small system *are*, in fact,
part of the
critical infrastructure. The Slammer worm proves the case.
Estimates of
the number of systems infected are on the order of 60-70,000.
This is
insignificant when compared to the hundreds of millions of
dedicated
machines on the net. Very few "critical infrastructure"
machines would have
been running the vulnerable system. However, the traffic
generated by the
infected machines affected every area of the Internet, plus many
private
systems. While SOHO systems may not be dedicated to
infrastructure
programs, their security can be just as important to the
functioning of the
infrastructure itself.

(Malicious software often creates problems for traditional
models and
understanding of security. I frequently point out to students
that viruses
present one of the few situations where the fact that *I* have
been
successfully attacked means that *you* have a problem.)

> DHS, in coordination with other agencies and private
organizations, will
> work to educate the general public of home users, students,
children, and
> small businesses on basic cyberspace safety and security
issues. As part
> of these efforts, DHS will partner with the Department of

Education and

- > state and local governments to elevate the exposure of cybersecurity
- > issues in primary and secondary schools. In addition, the Federal Trade
- > Commission will continue to provide information on cybersecurity for
- > consumers and small businesses through <http://www.ftc.gov/infosecurity>.

Again, this proposal sounds good, but, without details to back it up, I doubt that there will be any impact any time soon. If the government is concerned that there are not enough experts to help secure businesses, where are they going to find those who have not only the necessary security expertise, but the ability to translate the vital concepts to children?

- > DHS, in coordination with the Department of Education, will encourage and
- > support, where appropriate subject to budget considerations, state, local,
- > and private organizations in the development of programs and guidelines
- > for primary and secondary school students in cybersecurity. (A/R 3-2)

Subject to budget considerations. No further comment needed.

- > In recent years, with the spread of ``always on'' connections for systems,
- > such as cable modems, digital subscriber lines (DSL), and wireless and
- > satellite systems, the security of home user and small business systems
- > has become more important not only to the users themselves, but to others
- > to which they are connected through the Internet. For example, these
- > connections generally mean that larger amounts of data can be

sent and
> done so in a continuous stream. These two factors can be
exploited and
> used to attack other systems, possibly even resulting in
nationally
> significant damage. The Internet service providers, antivirus
software
> companies, and operating system/application software
developers that
> provide services or products to home users and small
businesses can help
> raise their awareness of cybersecurity issues.

What incentive do those companies have to do so? In many cases,
what
ability do they have to do so?

> Home users and small businesses can help the Nation secure
cyberspace by
> securing their own connections to it. Installing firewall
software and
> updating it regularly, maintaining current antivirus software,
and
> regularly updating operating systems and major applications
with security
> enhancements are actions that individuals and enterprise
operators can
> take to help secure cyberspace. To facilitate such actions,
DHS will
> create a public-private task force of private companies,
organizations,
> and consumer users groups to identify ways that providers of
information
> technology products and services, and other organizations can
make it
> easier for home users and small businesses to secure their
systems. (A/R
> 3-3)

"Make is easier." Such as, not using instant messaging and P2P
sharing
systems? Not using Outlook and IE? Turning off JavaScript and
ActiveX?

Not opening attachments? Foreswearing HTML formatted email?
And will the
companies promoting such technologies be likely to make such
recommendations?

> b. Large Enterprises

> The security of large enterprises is important not only to
individual
> businesses, but to the Nation as a whole. Large enterprises
own major
> cyber networks and computing systems that, if not secure, can
be exploited
> for attacks on other businesses in an increasingly
interconnected economy,
> and could, in the case of a massive attack, have major economic
> consequences. The cybersecurity of large enterprises can be
improved
> through strong management to ensure that best practices and
efficient
> technology are being employed, especially in the areas of
configuration
> management, authentication, training, incident response, and
network
> management. DHS will continue the work of sensitizing the
owners of these
> networks to their vulnerabilities and what can be done to
mitigate them.

How will they sensitize these owners? I suspect that the
strongest
encouragement will be successful lawsuits against companies that
failed to
secure themselves.

> DHS, working with other government agencies and private sector
> organizations, will build upon and expand existing efforts to
direct the
> attention of key corporate decision makers (e.g., CEOs and
members of
> boards of directors) to the business case for securing their
companies'
> information systems. Decision makers can take a variety of

steps to

- > improve the security of their enterprise networks and to ensure that their
- > networks cannot be maliciously exploited. Large enterprises are encouraged
- > to evaluate the security of their networks that impact the security of the
- > Nation's critical infrastructures. Such evaluations might include: (1)
- > conducting audits to ensure effectiveness and use of best practices; (2)
- > developing continuity plans which consider offsite staff and equipment;
- > and, (3) participating in industrywide information sharing and best
- > practice dissemination. (A/R 3-4)

Most of us in the security field would agree that a business case could be made for security. (After all, our jobs depend upon it.) However, most of us would also agree that such cases are not easy to put together. If the DHS can help put together such a case, it may help. But will this case be the usual one: vague, generic, and unconvincing? One grand business case for security overall will not help. Business cases too often have to be made on a protection system by policy by practice basis, and demand too much time (from those experts who are already, please note, in short supply).

- > i) Insider Threats. Many cyber attacks on enterprise systems are
- > perpetrated by trusted ``insiders.''
- > Insiders are people trusted with
- > legitimate access rights to enterprise information systems and
- > networks. Such trusted individuals can pose a significant threat to the
- > enterprise and beyond. The insider threat poses a key risk because it

- > provides a potential avenue for individuals who seek to harm the Nation to
- > gain access to systems that could support their malicious
- > objectives. Effectively mitigating the insider threat requires policies,
- > practices, and continued training. Three common policy areas which can
- > reduce insider threat include: (1) access controls, (2) segregation of
- > duties, and, (3) effective policy enforcement.

I'm not sure why the framers of this "strategy" chose to include this material in relation to education, although it does have some relevance.

- > . Poor access controls enable an individual or group to inappropriately
- > modify, destroy, or disclose sensitive data or computer programs for
- > purposes such as personal gain or sabotage.

Proper access controls require time and resources to determine, administer, and enforce. Remember those rare experts, again.

- > . Segregation of duties is important in assuring the integrity of an
- > enterprise's information system. No one person should have complete
- > control of any system.

Segregation of duties is remarkably difficult to teach. The dividing line between an operational function and an audit function is not immediately obvious in all cases.

- > . Effective enforcement of an enterprise security policy can be
- > challenging and requires regular auditing. New automated software is
- > beginning to emerge which can facilitate efficient enforcement of

> enterprise security. These programs allow the input of policy
in human
> terms, translation to machine code, and then monitoring at the
packet
> level of all data transactions within, and outbound from, the
> network. Such software can detect and stop inappropriate use
of networks
> and cyber-based resources.

Programs can help with the enforcement. The establishment of
the policy is
still as skilled task. We need help in training people skilled
in that
task.

> c. Institutions of Higher Education (IHEs)

> Awareness plays an especially important role in increasing the
> cybersecurity of IHEs. As recent experience has shown,
organized attackers
> have collectively exploited many insecure computer systems
traceable to
> the campus networks of higher education as a platform from
which to launch
> denial-of-service attacks and other threats to unrelated
systems on the
> Internet. Such attacks harm not only the targeted systems, but
also the
> owners of those systems and those who desire to use their
services. IHEs
> are subject to exploitation for two reasons: (1) they possess
vast amounts
> of computing power; and (2) they allow relatively open access
to those
> resources. The computing power owned by IHEs is extensive,
covering over
> 3,000 schools, many with research and significant central
computing
> facilities.

Good. DHS gonna spring for some money to help with the
administration of
security on college systems, or do the colleges have to take

resources away
from the task of educating students (perhaps in the art of
security?)?

> The higher education community, collectively, has been
actively engaged in
> efforts to organize its members and coordinate action to raise
awareness
> and enhance cybersecurity on America's campuses. Most notably,
through
> EDUCAUSE, the community has raised the issue of the Strategy's
development
> with top leaders of higher education, including the American
Council on
> Education and the Higher Education IT Alliance. Significantly,
through
> this effort, top university presidents have adopted a 5-point
Framework
> for Action that commits them to giving IT security high
priority and to
> adopting the policies and measures necessary to realize
greater system
> security:

Sounds interesting.

> (1) Make IT security a priority in higher education;

We've heard this before, from a variety of institutions.

> (2) Revise institutional security policy and improve the use
of existing
> security tools;

Uh huh ...

> (3) Improve security for future research and education
networks;

uh huh ...

> (4) Improve collaboration between higher education, industry,
and

> government; and

uh huh ...

> (5) Integrate work in higher education with the national effort to
> strengthen critical infrastructure.

Didn't you just say that?

> Colleges and universities are encouraged to secure their cyber systems by
> establishing some or all of the following as appropriate: (1) one or more
> ISACs to deal with cyber attacks and vulnerabilities; (2) model guidelines
> empowering Chief Information Officers (CIOs) to address cybersecurity; (3)
> one or more sets of best practices for IT security; and, (4) model user
> awareness programs and materials. (A/R 3-5)

We have heard this before. While I would agree that IHEs may be closer to the informed resources who can form such plans, I haven't seen that they are any closer to using them.

> d. Private Sectors

> DHS will work with private sectors on general awareness as well as on
> specific issues impacting particular sectors. Private sectors own and
> operate the vast majority of the Nation's cyberspace. As long time
> partners in the effort to secure cyberspace, many sectors have developed
> plans in parallel with the National Strategy to Secure Cyberspace to help
> secure their critical infrastructures. The sectors can serve a vital role
> in the reduction of vulnerabilities by creating sector-wide

awareness of

- > issues that affect multiple members. Members can develop and share best
- > practices and work together toward common security solutions. For example,
- > SCADA systems are a widespread security issue in the energy
- > sector. Solutions are being coordinated with the Department of Energy and
- > across the sector. The sectors also play a role in the identification of
- > research needs. DHS will closely coordinate with private sectors on plans
- > and initiatives to secure cyberspace.

As anyone who has been involved with security in the long term can attest, "vertical markets" can maintain some remarkably large blind spots. Forcing the sectors to have *outsiders* review their systems could be very beneficial.

- > A public-private partnership should continue work in helping to secure the
- > Nation's cyber infrastructure through participation in, as appropriate and
- > feasible, a technology and R&D gap analysis to provide input into the
- > federal cybersecurity research agenda, coordination on the conduct of
- > associated research, and the development and dissemination of best
- > practices for cybersecurity. (A/R 3-6)

This does not really appear to say much.

> e. State and Local Governments

- > DHS will implement plans to focus key decision makers in state and local
- > governments---such as governors, state legislatures, mayors, city
- > managers, and county commissioners/boards of supervisors---to

support

- > investment in information systems security measures and adopt enforceable
- > management policies and practices.

Focus or force?

> B. TRAINING

- > In addition to raising general awareness, the Nation must focus resources
- > on training a talented and innovative pool of citizens that can specialize
- > in securing the infrastructure. While the need for this pool has grown
- > quickly with the expansion of the Internet and the pervasiveness of
- > computers, networks, and other cyber devices, the investment in training
- > has not kept pace. Universities are turning out fewer engineering
- > graduates, and much of their resources are dedicated to other subjects,
- > such as biology and life sciences. This trend must be reversed if the
- > United States is to lead the world with its cyber economy.

I suspect that this comment relates only to training about info tech in general. The level of training in infosec, we all know, is far less.

> 1. Foster Adequate Training and Education Programs to Support the Nation's
> Cybersecurity Needs

- > Improvements in cybersecurity training will be accomplished primarily
- > through the work of private training organizations, institutions of
- > learning, and the Nation's school systems. DHS will also encourage private
- > efforts to ensure that adequate opportunities exist for

continuing

- > education and advanced training in the workplace to maintain high skills
- > standards and the capacity to innovate.

Did we not foresee this? "It's your responsibility, not ours."

Some

strategy.

> The federal government can play a direct role in several ways.

First, DHS

- > will implement and encourage the establishment of programs to advance the
- > training of cybersecurity professionals in the United States, including
- > coordination with NSF, OPM, and NSA, to identify ways to leverage the
- > existing Cyber Corps Scholarship for Service program as well as the
- > various graduate, postdoctoral, senior researcher, and faculty development
- > fellowship and traineeship programs created by the Cyber Security Research
- > and Development Act, to address these important training and education
- > workforce issues. (A/R 3-7)

Sounds interesting. Needs development. Show your work. C-

> 2. Increase the Efficiency of Existing Federal Cybersecurity Training

> Programs

> Second, DHS will explore the benefits of a center for the development of

- > cybersecurity training practices that would draw together expertise and be
- > consistent with the federal ``build once, use many'' approach.

DHS, in

- > coordination with other agencies with cybersecurity training expertise,
- > will develop a coordination mechanism linking federal cybersecurity and

> computer forensics training programs. (A/R 3-8)

Linking? How about funding?

> C. CERTIFICATION

> 1. Promote Private Sector Support for Well-coordinated Widely Recognized

> Professional Cybersecurity Certifications

> Related to education and training is the need for certification of

> qualified persons. Certification can provide employers and consumers with

> greater information about the capabilities of potential employees or

> security consultants. Currently, some certifications for cybersecurity

> workers exist; however, they vary greatly in the requirements they

> impose. For example, some programs emphasize broad knowledge verified by

> an extensive multiple-choice exam, while others verify in-depth practical

> knowledge on a particular cyber component. No one certification offers a

> level of assurance about a person's practical and academic qualifications,

> similar to those offered by the medical and legal professions.

I note that the emphasis on academic qualifications, while weakened from the

initial draft, still exists. I would agree that many security "experts"

would benefit from the rigour of more formal study. However, many academics

would also benefit from practical experience. I suspect that the needs of

security certification do not always require a degree.

I rather suspect that a security "profession," along the lines of the

medical and legal, is not going to happen.

- > To address this issue, a number of industry stakeholders including
- > representatives of both consumers and providers of IT security
- > certifications are beginning to explore approaches to developing
- > nationally recognized certifications and guidelines for certification.

- > Aspects that warrant consideration by these organizations include levels
- > of education and experience, peer recognition, continuing education
- > requirements, testing guidance, as applicable for various levels of
- > certification that may be established, and models for administering a
- > certification for IT security professionals similar to those successfully
- > employed in other professions. DHS and other federal agencies, as
- > downstream consumers (prospective employers of certified personnel), can
- > aid these efforts by effectively articulating the needs of the federal IT
- > security community. DHS will encourage efforts that are needed to build
- > foundations for the development of security certification programs that
- > will be broadly accepted by the public and private sectors. DHS and other
- > federal agencies can aid these efforts by effectively articulating the
- > needs of the federal IT security community. (A/R 3-9)

OK, the government doesn't want to help or fund certification, but wants to dictate what the certification is for.

Most of the following "action items" have already been addressed in the foregoing:

> Priority III: A National Cyberspace Security Awareness and Training Program

> A/R 3-1: DHS, working in coordination with appropriate federal, state, and

> local entities and private sector organizations, will facilitate a

> comprehensive awareness campaign including audience-specific awareness

> materials, expansion of the StaySafeOnline campaign, and development of

> awards programs for those in industry making significant contributions to

> security.

> A/R 3-2: DHS, in coordination with the Department of Education, will

> encourage and support, where appropriate subject to budget considerations,

> state, local, and private organizations in the development of programs and

> guidelines for primary and secondary school students in cybersecurity.

> A/R 3-3: Home users and small businesses can help the Nation secure

> cyberspace by securing their own connections to it. Installing firewall

> software and updating it regularly, maintaining current antivirus

> software, and regularly updating operating systems and major applications

> with security enhancements are actions that individuals and enterprise

> operators can take to help secure cyberspace. To facilitate such actions,

> DHS will create a public-private task force of private companies,

> organizations, and consumer users groups to identify ways that providers

> of information technology products and services, and other organizations

> can make it easier for home users and small businesses to

secure their
> systems.

I imagine AV and firewall vendors will be delighted that the government will be advertising for them.

> A/R 3-4: Large enterprises are encouraged to evaluate the security of
> their networks that impact the security of the Nation's critical infra-
> structures. Such evaluations might include: (1) conducting audits to
> ensure effectiveness and use of best practices; (2) developing continuity
> plans which consider offsite staff and equipment; and, (3) participating
> in industrywide information sharing and best practices dissemination.

> A/R 3-5: Colleges and universities are encouraged to secure their cyber
> systems by establishing some or all of the following as appropriate: (1)
> one or more ISACs to deal with cyber attacks and vulnerabilities; (2)
> model guidelines empowering Chief Information Officers (CIOs) to address
> cybersecurity; (3) one or more sets of best practices for IT security;
> and, (4) model user awareness programs and materials.

> A/R 3-6: A public-private partnership should continue work in helping to
> secure the Nation's cyber infrastructure through participation in, as
> appropriate and feasible, a technology and R&D gap analysis to provide
> input into the federal cybersecurity research agenda, coordination on the
> conduct of associated research, and the development and dissemination of
> best practices for cybersecurity.

- > A/R 3-7: DHS will implement and encourage the establishment of programs to
- > advance the training of cybersecurity professionals in the United States,
- > including coordination with NSF, OPM, and NSA, to identify ways to
- > leverage the existing Cyber Corps Scholarship for Service program as well
- > as the various graduate, postdoctoral, senior researcher, and faculty
- > development fellowship and traineeship programs created by the Cyber
- > Security Research and Development Act, to address these important training
- > and education workforce issues.

- > A/R 3-8: DHS, in coordination with other agencies with cybersecurity
- > training expertise, will develop a coordination mechanism linking federal
- > cybersecurity and computer forensics training programs.

- > A/R 3-9: DHS will encourage efforts that are needed to build foundations
- > for the development of security certification programs that will be
- > broadly accepted by the public and private sectors. DHS and other federal
- > agencies can aid these efforts by effectively articulating the needs of
- > the Federal IT security community.

rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

<http://victoria.tc.ca/techrev> or <http://sun.soci.niu.edu/~rslade>

IEEE Symposium on Security and Privacy

Lee Badger <lbadger@darpa.mil>

Tue, 11 Mar 2003 08:42:28 -0500

Lee Badger, Program Manager, Information Processing Technology
Office

DARPA voice: 571.218.4327 fax: 703.248.1879

2003 IEEE Symposium on Security and Privacy, PRELIMINARY
PROGRAM

May 11-14, 2003, The Claremont Resort, Oakland, California, USA
sponsored by IEEE Computer Society Technical Committee on
Security and Privacy in cooperation with
The International Association for Cryptologic Research (IACR)
For more information, see www.ieee-security.org/TC/SP-Index.html

Monday MORNING

Anonymity:

Mixminion: Design of a Type III Anonymous Remailer Protocol

George Danezis (Cambridge Univ.), Roger Dingledine, Nick
Mathewson (Free Haven Project)

Probabilistic Treatment of MIXes to Hamper Traffic Analysis

Dakshi Agrawal (IBM Watson), Dogan Kesdogan, Stefan Penz
(Aachen
Univ. Tech.)

Defending Anonymous Communication Against Passive Logging Attacks

Matt Wright, Micah Adler, Brian Neil Levine, Clay Shields
(U. Mass.)

Intrusion Detection:

Active Mapping: Resisting NIDS Evasion Without Altering Traffic

Umesh Shankar (UC Berkeley), Vern Paxson (ICSI)

Anomaly Detection Using Call Stack Information

Henry Hanping Feng (U. Mass.), Oleg M. Kolesnikov, Prahlad
Fogla,
Wenke Lee (Georgia Tech.), Weibo Gong (U. Mass.)

Monday AFTERNOON

Invited talk

Operating Systems:

Defending Against Denial-of-Service Attacks with Puzzle Auctions

XiaoFeng Wang, Mike Reiter (CMU)

Pi: A Path Identification Mechanism to Defend against DDoS Attacks

Abraham Yaar, Adrian Perrig, Dawn Song (CMU)

5-minute talks

Tuesday MORNING

Formal Methods:

A Unified Scheme for Resource Protection in Automated Trust Negotiation

Ting Yu, Marianne Winslett (U. Illinois, Urbana-Champaign)

Beyond Proof-of-compliance: Safety and Availability Analysis in Trust

Management

Ninghui Li (Stanford), William H. Winsborough (NAI Labs), John

C. Mitchell (Stanford)

Intransitive Non-Interference for Cryptographic Purposes

Michael Backes, Birgit Pfitzmann (IBM Zurich)

Hardware:

Specifying and Verifying Hardware for Tamper-Resistant Software

David Lie, John Mitchell (Stanford), Chandramohan Thekkath (Microsoft Research), Mark Horowitz (Stanford)

Using Memory Errors to Attack a Virtual Machine

Sudhakar Govindavajhala, Andrew W. Appel, (Princeton)

Tuesday AFTERNOON

Invited talk

Hardware & Crypto:

Secret Handshakes from Pairing-Based Key Agreements

D. Balfanz, G. Durfee (PARC), N. Shankar (U. Maryland),

D.K. Smetters, J. Staddon, H.C. Wong (PARC)

Random Key Predistribution Schemes for Sensor Networks

Haowen Chan, Adrian Perrig, Dawn Song (CMU)

Wednesday MORNING

Distributed Systems:

Hardening Functions for Large Scale Distributed Computations

Douglas Szajda, Barry Lawson, Jason Owen (U. Richmond)

A Practical Revocation Scheme for Broadcast Encryption Using Smart Cards

Noam Kogan, Yuval Shavitt, Avishai Wool (Tel Aviv Univ.)

Using Replication and Partitioning to Build Secure Distributed Systems

Lantian Zheng, Stephen Chong, Andrew C. Myers (Cornell),
Steve

Zdancewic (U. Pennsylvania)

Vulnerabilities in Synchronous IPC Designs

Jonathan S. Shapiro (Johns Hopkins)

Garbage Collector Memory Accounting in Language-Based Systems

David W. Price, Algis Rudys, Dan S. Wallach (Rice)



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

[ACM](#) Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 64

Tuesday 18 March 2003

Contents

- [Apparently uncommanded rudder movement injures cruise passengers](#)
[Steve Peterson](#)
- [Jeppesen GPS navigation database corruption](#)
[Mickey Coggins](#)
- [California outage causes prescription mix-up](#)
[Richard Cook](#)
- [Glitch let gamblers beat machines](#)
[M Taylor](#)
- [Haywire ATM spits out extra cash](#)
[Fuzzy Gorilla](#)
- [Beware the spelling checker](#)
[NewsScan](#)
- [Recent worms punish bad passwords](#)
[David J. Aronson](#)
- [Profile of a virus writer](#)
[NewsScan](#)
- [Search engines making sensitive information easy to locate](#)
[Richard Moore](#)
- [Benetton clothes to include tracking chip](#)
[Monty Solomon](#)

- [CASPIAN calls for immediate worldwide boycott of Benetton](#)
[Monty Solomon](#)
 - [Federated network identity](#)
[Brian Seborg](#)
 - [Re: Computer crashes threaten hospital operations](#)
[Jonathan Kamens](#)
 - [Re: Monster electricity bill](#)
[Don Gingrich](#)
 - [Human protocol failure](#)
[Dawn Cohen](#)
 - [The Workshop on Rapid Malcode: WORM](#)
[Robert K. Cunningham](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✂ **Apparently uncommanded rudder movement injures cruise passengers**

Steve Peterson <steve@zpf.com>
Mon, 17 Mar 2003 11:52:03 -0600

I received an e-mail from relatives who are on a Holland America cruise around the tip of South America. Last Thursday night, while they were eating dinner in the dining room, there was a sudden lurch and the ship went into a hard right turn, listing over at an estimated angle of 20 degrees. Every chair in the dining room toppled and people, dishes and food slid everywhere. At least two people were injured in the laundry when clothes dryers toppled on top of them. The grand piano on the stage was flipped over.

After about 5 minutes, the ship stopped turning. Shortly after

that, the captain came on the PA system and announced that, when they turned off the autopilot to enter the port at Buenos Aires, the rudder swung to the right and could not be "unstuck." Over two hours elapsed after the incident, before the crew performed a count of the passengers.

✶ Jeppesen GPS navigation database corruption

Mickey Coggins <risks-spam-alert@int.ch>

Fri, 14 Mar 2003 17:53:25 +0100

I just got this from the AOPA (Aircraft Owners and Pilots Association), a truly outstanding organization, BTW.

Jeppesen reports airspace boundary problems

About 350 airspace boundaries contained in Jeppesen NavData are incorrect,

the FAA has warned. The error occurred at Jeppesen after a software

upgrade when information was pulled from a database containing 20,000

airspace boundaries worldwide for the March NavData update, which takes

effect March 20. Only a dozen are in the United States, including Chicago;

Louisville, Kentucky; Fayetteville, North Carolina; Santa Ana, California;

Las Vegas; Honolulu; Des Moines; and Oklahoma City. The error could cause

pilot alerts to be given by GPS units too early or too late. Pilots are

advised to use multiple sources of information, such as carrying paper

charts (Jeppesen paper charts are unaffected by the problem),

and
contacting controlling agencies by radio to avoid airspace
violations. Jeppesen has provided a searchable database of
locations with
airspace boundary errors on its Web site (
<http://www.aopa.org/epilot/redirect.cfm?adid=1875>). To search,
click on the
binocular icon and enter an airport identifier. Jeppesen
spokesman Mike
Pound said the errors will be corrected "for the next possible
release."
The next release is scheduled for April 17.

The risks are pretty obvious. Today if you fly your tiny
aircraft into
restricted airspace in the USA, you can get shot down by agents
of "The
Department of Homeland Security".

Many (most) pilots use this navigation data with their GPS as
their primary
source of navigation information worldwide.

Please don't get me started on the absurdity of many of these
airspace
restrictions in the first place...

California outage causes prescription mix-up

"Richard Cook" <ri-cook@uchicago.edu>
Tue, 18 Mar 2003 09:58:16 -0600

Thousands of patients could have received the wrong prescription
drugs after
a power outage at Kaiser Permanente's computer center in
Southern California
knocked the pharmacy's labeling system out of sync -- printing
the wrong

labels on filled prescriptions. There were no reports yet of patients suffering from adverse reactions. About 4,700 patients from Fresno to the Oregon border were affected, including those ordering prescriptions by telephone. After the error was discovered on 14 Mar 2003, hospital officials attempted to contact the affected patients, although by 17 Mar, 152 remained uncontacted -- including those for whom they had only PO-box addresses. [Source: Associated Press, 18 Mar 2003, PGN-ed; Also noted by Danny Burstein]

✂ Glitch let gamblers beat machines

M Taylor <mctaylor@privacy.nb.ca>

Thu, 13 Mar 2003 12:50:34 +0000

Some Nova Scotia video lottery terminal (VLT) players found a way to beat machines last year, forcing the Atlantic Lottery Corp. to replace computer chips in about one-third of their 3,538 VLTs in Nova Scotia and Newfoundland. About 20 locations appeared to have had the glitch exploited. ALC doesn't know how much it lost, but noted the maximum payout for a single spin is \$500. The problem was discovered in December 2002 after ALC received calls from retailers who noticed frequent high payouts, and from its own inspections. Chips were replaced in January and February 2003. [Glitch let gamblers beat machines, *The Chronicle-Herald*, Nova Scotia, 8 Mar 2003; PGN-ed]

<http://www.herald.ns.ca/>

M Taylor <http://www.mctaylor.com/>

⚡ Haywire ATM spits out extra cash

"Fuzzy Gorilla" <fuzzygorilla@euroseek.com>

Fri, 14 Mar 2003 18:54:43 -0500

Several bank customers in Fargo, North Dakota, had an automated teller machine dispense more cash than they had requested. (They turned it in.)

Apparently ``cold weather caused the ATM cash door to stick so some

customers who wanted to withdraw money could not get it. The door opened

for other customers, who then wound up with their cash and the cash

belonging to the previous customers.' ' [Source: AP, 14 Mar 2003; PGN-ed]

<http://story.news.yahoo.com/news>

?tmpl=story2&u=/ap/20030314/ap_on_fe_st/haywire_atm

⚡ Beware the spelling checker

"NewsScan" <newsscan@newsscan.com>

Mon, 17 Mar 2003 09:42:19 -0700

A study at the University of Pittsburgh reveals that the ubiquitous spelling checker software may be doing as much harm as good, when it comes to

writing. In the study, 33 undergraduate students were asked to proofread a one-page business letter -- half of them using Microsoft Word, with its spelling- and grammar-checking features and the other half using only their brains. Without the software, students with higher SAT verbal scores made, on average, five errors, compared with 12.3 errors made by students with lower scores. However, using the software, the two groups made about the same number of errors -- 16 vs 17. Dennis Galletta, a professor of information systems at the Katz Business School, says people have come to rely on spelling-checker software too completely. "It's not a software problem, it's a behavior problem." [AP 14 Mar 2003; NewsScan Daily, 17 March 2003; slight PGN-ed]

<http://apnews.excite.com/article/20030314/D7POQ7R80.html>

Recent worms punish bad passwords

"David J. Aronson" <dja2003@hotpop.com>

Tue, 11 Mar 2003 10:20:36 -0500

A spike in Internet traffic caused by a worm over the weekend can be

largely blamed on bad passwords and poor security practices, said security

experts on Monday. The Deloder worm, which spreads by communicating with

Windows computers that have file sharing enabled, may have spread to

perhaps as many as 10,000 systems using a list of 86 passwords to break

into computers running Microsoft Windows NT, 2000 and XP.

[Source: MSNBC]

<http://www.msnbc.com/news/883415.asp>:

The same article later says:

The recent LovGate worm -- which appeared on the Internet two weeks ago --

uses a list of 16 passwords as a secondary way to infect computers.

Yet another RISK of bad password choices. And before PGN says it:

Deloder attacked de losers! B-)

David J. Aronson, Software Engineer for hire in Washington DC area.

See <http://destined.to/program/> for online resume, references, etc.

Profile of a virus writer

"NewsScan" <newsscan@newsscan.com>

Tue, 18 Mar 2003 09:03:24 -0700

According to the UK's Sophos, one of the world's largest antivirus companies, about 1,000 viruses are created every month, and in almost all cases the perpetrators are computer-obsessed males between the ages of 14 and 34. "They have a chronic lack of girlfriends, are usually socially inadequate and are drawn compulsively to write self-replicating codes. It's a form of original graffiti to them," says Sophos CEO Jan Hruska. Virus writers tend to explore known bugs in existing software or look

for vulnerabilities in new versions in order to create and spread their infections, and Hruska notes that the next target for the virus writing community could be Microsoft's .Net platform for Web services. To boost the impact of their creations, virus writers also tend to share information to create variants of the same infection, such as the infamous Klez worm, which has been among the world's most prolific viruses in the last year.

[Reuters/CNet News.com 18 Mar 2003; NewsScan Daily, 18 March 2003]

http://news.com.com/2100-1002-993023.html?tag=fd_top

🔥 Search engines making sensitive information easy to locate

Richard Moore <rich@westpoint.ltd.uk>

Thu, 13 Mar 2003 11:53:32 +0000

I work for a company that performs vulnerability assessment using tools such as the nessus security scanner. Yesterday I was searching for more information about one of the security holes in a report, and I came across someone else's report with the same hole. Looking a bit further, I noticed that searching for 'nessus report' I got a dozens of pages back. Some of the pages returned were sample reports from companies like ours (or the nessus site itself), but others were from people who had left their reports in location visible to search engines.

The danger here is obvious - do you really want to make a list of all your security holes visible to the world? Things are actually even worse than they first appear too, because engines like google cache the pages, so even if you delete them people can still access the information.

✶ Benetton clothes to include tracking chip

Monty Solomon <monty@roscom.com>

Wed, 12 Mar 2003 13:06:07 -0500

Clothes sold at Benetton stores will soon contain microchip transmitters that allow the Italian retailer to track its garments from their point of manufacture to the moment they're sold in any of its 5,000 shops.

[Source: Associated Press, 11 Mar 2003]

<http://news.lycos.com/news/story.asp?section=Business&storyId=673780>

Tag, You're It: What Your Clothes Say About You

Clothing designer Benetton plans to weave radio frequency ID chips

into its garment tags. While Benetton is poised to save money by tracking the clothes with RFID, it could also mean a loss of customers' privacy. [Source: Elisa Batista, wired.com]

<http://www.wired.com/news/wireless/0,1382,58006,00.html>

✶ CASPIAN calls for immediate worldwide boycott of Benetton

Monty Solomon <monty@roscom.com>

Wed, 12 Mar 2003 18:53:33 -0500

An American consumer privacy group has called for an immediate, worldwide
boycott of Benetton, following disclosures that the company has placed
identification and tracking devices into its clothing products.
CASPIAN

(Consumers Against Supermarket Privacy Invasion and Numbering)
announced
that it will oppose Benetton's plans to place Radio Frequency
Identification
(RFID) chips into clothing labels intended for the consumer
market.

For additional information, see Phillips/Benetton press release:
http://biz.yahoo.com/bw/030311/115697_1.htm

Forbes article illustrating remote inventorying of shoppers'
clothing

(As reproduced on Alien Technology's Web site)

http://www.alientechnology.com/news/The_Internet_of_Things.htm

CASPIAN overview of privacy concerns associated with RFID
technology:

<http://www.nocards.org/AutoID/overview.shtml>

⚡ Federated network identity

"brian-h seborg" <brian.seborg@telispark.com>

Tue, 18 Mar 2003 17:57:55 -0500

One of the "Holy Grails" of networking has long been the concept
of single

sign-on. For those not familiar with the term, it refers to the
ability for

a user to authenticate once to some authentication server and
then to have

access to many different systems in a secure but unimpeded

manner. Kerberos includes the concept of single sign-on within its framework as does DCE. X.509 certificates and associated PKI also hold forth the concept of single-sign-on through the use of certificates that are issued by a trusted issuing authority, and can be presented as a means of authenticating the user. More recently, Microsoft has come up with a Web-based identity in their Microsoft Passport standard. A competing standard to Microsoft Passport is that being put forth by the Liberty Alliance Project. In all of the standards above, there is the concept of users having a set of attributes or credentials associated with their authenticated identity. These credentials can be used to determine whether or not users should have access to certain systems, and, further, to determine the level of access. The attributes can also include such things as age verification, credit card information, address, etc. that could be used with on-line merchants for purchase or other purposes. However, as this concept has matured, there is now the thought that users would be able to have (Microsoft Passport and Liberty Alliance), a single federated network identity, and that the user would have some control over what information he would be willing to share with different communities (e.g., a user could have a work profile associated with his ID that would provide certain salient information to work related computers and a home profile that would provide potentially different information to computers that the same user accesses from home).

The ability to have such a federated network identity would, if it could be administered in a secure fashion, enable any Web site or Web application that accepted the federated identity (once authenticated by an identity provider) to have a clear idea of whom they are dealing with. In other words, rather than Joe Smith connecting to a site as Joe Smith, JSmith, Jdog, etc. and appearing to be one or multiple users, he would be Joe Smith always. Now, as you can imagine, the ability of Joe to be able to determine what information he wants to share with different sites would be important. For example, Joe may be quite willing to share his full name, mailing address, and credit card number with an on-line store, but only be willing to share his age with a porn site that may be allowing free tours to prospective customers who can provide age verification. The problem is, that, as we have seen with the misuse of social security numbers by other than the Social Security Administration in the U.S., we can expect to see sites demanding more information than they legitimately need in order to allow access. So, this places the burden (and perhaps rightly so) on the individual to make sure that he makes good choices as to what information he is willing to share with each community. This may be quite a bit to expect of someone who is not technically savvy enough to understand the ramifications of these choices. This risk can be mitigated to an extent by looking to a third party to help an individual reduce some of this risk. For example, if I connect to a portal provided by my bank and the bank

performs the identity verification to ensure that I am who I say I am, then I may assume that any vendors that look to the bank to verify my identity and associated credentials have, themselves, been scrutinized by the bank and determined to be trustworthy at least to the extent that they have privacy policies that are similar to that of the banks so that information provided to them is treated with the same care as that provided to the bank. Unfortunately, I think this is contrary to reality. So, the point is, be very suspicious of Microsoft Passport or of the Liberty Alliance Project, or any other group who is trying to create the equivalent of a universal ID. While I think that they have some very good ideas, and are trying to create a federated network identity with the best of intentions, there is much that is not being covered that may call for not only study by consumer groups, but for legislation and additional infrastructure. Even then, I would still want to be able to anonymously surf the Web the same way I anonymously enter stores at the mall, knowing that I can walk in, look around and even purchase something without the store knowing who I am.

✶ Re: Computer crashes threaten hospital operations (Solomon, [R-22.62](#))

Jonathan Kamens <jik@kamens.brookline.ma.us>
Tue, 11 Mar 2003 13:04:29 -0500

As far as I could tell from the article, what happened at Beth Israel Deaconess in November 2002 [year fixed in RISKS ARCHIVES. PGN-oops] was not a "computer crash." That's one of the terms that journalists use when they either don't understand what went wrong or are trying to dumb it down for the semi-literate masses.

Quoting from *The Boston Globe* article, "The computer crash at Beth Israel occurred when a research [sic] flooded the network with large quantities of data, causing the strained system to slow drastically.... networks must have sufficient bandwidth and modern routing systems, and should allow for portions to be shut down without the system becoming disabled."

In other words, the network didn't have enough bandwidth to handle the traffic being thrown at it, there was no infrastructure in place for limiting the amount of bandwidth used by individual computers or applications, there was no infrastructure in place for monitoring bandwidth in real-time to detect anomalies and trace them to their sources, and there was no infrastructure in place for reactively locating high bandwidth consumers.

For all of these things to be missing in a mission-critical network is shocking (and that's why the articles about it were written), but not terribly surprising. Beth Israel Deaconess has been in dire financial straits for several years; I doubt they pay high enough salaries to attract the best and brightest IT professionals, people who understand the

importance of constructing a robust network and how to go about doing it. I also doubt they've budgeted enough money to be able to afford the proper infrastructure; perhaps, after last November's outage, that will change.

✈ Re: Monster electricity bill ([RISKS-22.61-62](#))

gingrich <gingrich@bigpond.net.au>
Fri, 14 Mar 2003 07:43:05 +1100

I can comment in some detail about a similar situation.

I worked for what was the State Electricity Commission of Victoria (Australia) in the early 1990s. A new customer billing system was implemented which, among other things included a "special" interface for senior billing officers in each local office that bypassed most of the sanity checks in the system, and allowed the sanity checks to be over-ridden, if necessary.

The electricity meter was replaced for a customer and this was not correctly recorded. Then when the next, regularly scheduled meter reading was entered into the system, it looked as if the meter had gone from a low value to an even lower value. This resulted in an enormous bill, a significant percentage (about 10%, from memory) of total sales for the district.

The system asked for confirmation, but the operator (an ordinary data entry

clerk, not the supervisor) thoughtlessly confirmed the entry. Since it was "special" mode the transaction was confirmed.

The customer received a bill for several million Australian dollars.

The risks?

Creating data entry screens with the power to gratuitously override the sanity checks for the data that are built into the system.

Is this really a direct problem with the computer system? I'm not sure. It is definitely a problem with the interaction between the computer system and the organisational systems designed to use the computer system.

The real lesson is that there is a need to recognise that computer systems do not exist in isolation, and that giving the power to override the system to ordinary users is a bad idea.

Don Gingrich gingrich@cs.rmit.edu.au School of CSIT, RMIT
Melbourne, Au

[New meters and wrap-arounds are of course old problems. For example, see [RISKS-7.40](#) and [RISKS-12.16](#). PGN]

⚡ Human protocol failure

"Dawn Cohen" <COHEND@wyeth.com>
Tue, 11 Mar 2003 16:40:21 -0500

I guess I'm a bit influenced by RISKS, and observed a disturbing

(human-based) protocol failure last week in my daughter's after school care.

I think it would come down to one of those system-boundary things.

On a normal day, my daughter goes to school on the school bus, but after school, she attends an after school program physically located in the school, but administered by the local YWCA. I pick her up from the school.

Transfer of daughter among three parties: school bus -> school -> YWCA.

Last week, we had one of those days that we were being threatened with a snowstorm (early news reports promised 3-6 inches by afternoon), and this being New Jersey, everyone panicked.

Because there was ultimately no serious accumulation of snow, everything was business-as-usual for most of the day. However, at 2:00, I got a phone call from the after school program, indicating that the program would not be available that afternoon, due to the snow, and that I should pick my daughter up. I arrived at the school at 3:00, and was herded into the cafeteria, to wait with the other anxious and disoriented after school program parents, for the 3:10 dismissal. At 3:10, children began filtering into the cafeteria, and parents collected their children and left. 10 minutes later, half a dozen parents remained, and we were informed by a teacher that all of the non-bus children had been released. She said that the Y had told the school to put all the after school program children onto the school bus. At that point, I ran out, and with some

difficulty located
the school bus that my daughter comes to school on (which had
luckily not
pulled out, yet), and pulled her off the bus.

System risks here:

- 1) The school accepts YWCA's word that it has informed all
parents of
the closure of the after-school program (what if the Y had
not been able
to reach me?)
- 2) The school accepts YWCA's word that it has informed all of the
parents of what action will be taken (this failed in my case)
- 3) The school releases my child to a 3rd party (the school bus)
that does
not have sufficient information for the situation. The
school has
emergency contacts for me and alternative pick-up people, as
does the
afterschool program. The school bus department does not have
this
information. It was not clear what the bus driver would have
done if I
had not rescued my daughter. I asked him what would have
happened if he
tried to drop my daughter at the house, with nobody at home,
and it seems
like their protocol is the most sensible: if there is no one
to receive a
child, radio the transportation department. The department
then calls
the home (the only number they have for me), and if no one
answers, take
the child back to school. If I want my neighbors to take my
child, I
have to supply a note to this effect.

I don't know. Maybe I'm just refusing to take off my RISKS
glasses, here,
but I think there's problems in the protocol with all three
parties. I've
communicated with the Principal, who refuses to accept any
responsibility.

She asserts that the whole fault is with the Y, who should have informed me that my daughter would be sent home on the bus. Personally, from reading RISKS, I think it is unacceptable to assume that communication was sent correctly to all parents. The school explicitly demands at the beginning of the year a list of acceptable people to release my child to, and the school bus is not on this list. I guess a better protocol would require the Y to provide minimal coverage at the school until such time as any parents who have not been successfully contacted arrive. Also, I guess I'm going to have to suggest that the transportation department keep my emergency contacts list, too.

🚩 Announcement: The Workshop on Rapid Malcode: WORM

"Robert K. Cunningham" <rkc@ll.mit.edu>

Tue, 18 Mar 2003 17:00:38 -0500

The Workshop on Rapid Malcode (WORM)
Workshop held in association with the
10th ACM Conference on Computer and Communications Security,
October 27th, 2003 Washington D.C.
Call for Papers

In the last several years, Internet-wide infectious epidemics have emerged as one of the leading threats to information security and service availability. The vehicle for these outbreaks, malicious codes called "worms", leverage the combination of software monocultures and the uncontrolled Internet communication model to quickly compromise

large numbers of hosts. Current operational practices have not been able to manage these threats effectively and the research community is only now beginning to address this area. The goal of this workshop is to bring together ideas, understanding and experience bearing on the worm problem from a wide range of communities including academia, industry and the government. We are soliciting papers from researchers and practitioners on subjects including, but not limited to:

- Modeling and analysis of propagation dynamics
- Automatic detection, characterization, and prediction
- Analysis of worm construction, current & future
- Propagation strategies (fast & obvious vs slow and stealthy)
- Reactive countermeasures
- Proactive defenses
- Threat assessment
- Forensic methods of attribution
- Significant operational experiences

Paper submissions due 1 Jul 2003; submission instructions will appear at

<http://pisa.ucsd.edu/worm03/>

General Chair: Stuart Staniford, Silicon Defense

Publicity Chair: Robert Cunningham, MIT Lincoln Lab

Program Committee Chair: Stefan Savage, UC San Diego

Program Committee Members: Robert Cunningham, MIT Lincoln Lab;

Anup Ghosh, DARPA; David Moore, CAIDA/UC San Diego;

Carey Nachenberg, Symantec; Vern Paxson, ICIR/LBL;

Phil Porras, SRI; Jeff Rowe, UC Davis; Mike Skroch, Sandia;

Stuart Staniford, Silicon Defense; Don Towsley, UMassAmherst

Dr. Robert K. Cunningham, Information Systems Technology Group
MIT Lincoln Laboratory <http://www.ll.mit.edu/IST/>



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

[ACM](#) Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 65

Friday 28 March 2003

Contents

- [Autotote betting scam sentencing](#)
[PGN](#)
- [Patriot software again a concern?](#)
[James Paul](#)
- [Surveillance Nation](#)
[Monty Solomon](#)
- [U.S. lifts FBI criminal database checks](#)
[Peets](#)
- [Text message disables Siemens mobile phones](#)
[Derek K. Miller](#)
- [Wireless mushrooms](#)
[Brian H. Seborg](#)
- [Failure of aircraft electronic displays at a critical moment](#)
[Peter B. Ladkin](#)
- [A320 incident partly due to computer failure](#)
[Peter B. Ladkin](#)
- [Paper is good](#)
[David Magda](#)
- [FTC's National Telemarketing "Do Not Call" Web Site to Launch 1 Jul](#)
[CDT Info](#)

- [Transient Microsoft Passport security vulnerability](#)
[James Van Bokkelen](#)
 - [Re: Traffic lights don't work in the snow](#)
[Ryan O'Connell](#)
 - [Re: Beware the spelling checker](#)
[Crispin Cowan](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Autotote betting scam sentencing

"Peter G. Neumann" <neumann@csl.sri.com>
Fri, 21 Mar 2003 11:08:57 PST

```
Auto-tote that charge,  
  and lift that trail,  
Get a little bunk-o,  
  and you land in jail.
```

[Apologies to "Old Man <up the> River"]

In [RISKS-22.33](#) and [22.38](#) through [22.40](#), we discussed the case of the former Autotote programmer who hacked the Catskill NY off-track horse-race betting system (which had a very weak audit trail), resulting in a rigged \$3 million winning Breeders' Cup Pick Six bet, plus other previous scams, on which his two Drexel frat buddies collected the winnings. The sentences have now been handed down. Programmer Chris Harn was given the minimum possible jail time -- only a year and a day instead of "up to seven years" -- because he "helped" the authorities; his frat buddies were given two- and three-year terms. [Source: *San Francisco Chronicle* item, 21 March 2003]

I suppose one of the tabloids might find a cute headline such as

Fat-cat frat rat begat rat-a-tat automat reformat, sat pat.
Splat!

⚡ Patriot software again a concern?

<james.paul@mail.house.gov>

Wed, 26 Mar 2003 01:58:13 -0500 (EST)

"For the second time in as many days, a U.S. Patriot missile defense battery has apparently locked its sights on an allied fighter plane, raising concern about a potentially serious glitch in the system's targeting software." A Patriot system about 30 miles south of Najaf in Iraq apparently locked on to an Air Force F-16 fighter on 24 Mar, and prepared to fire. The F-16 responded by firing a high-speed anti-radiation HARM missile at the battery, destroying its radar dish. This came a day after a Patriot missile shot down a British Royal Air Force Tornado GR4 fighter near the Kuwaiti border, killing both crew members. The British fliers were the first known friendly fire casualties of the war in Iraq. [There was discussion about whether to blame the Patriot software or the system operators, although evidence seems to favor the former.] [Source: Jonathan Weisman, *The Washington Post*, 25 Mar 2003; PGN-ed]

<http://www.washingtonpost.com/wp-dyn/articles/A29390-2003Mar25.html>

[The Patriot of course had a checkered role in the 1991 Persian Gulf War, with initial reports of great success, followed by official reports that it was only about 10% successful. But after three major upgrades, it is now thought to be much better, having knocked out 6 of 14 Iraqi missiles.
PGN]

[Incidentally, NBC on 24 Mar 2003 had an item on self-inflicted damage, noting that in the Vietnam War, 24% of U.S. fatalities were due to friendly fire. I have heard reports that it was even higher in the first Gulf War. That is truly astounding! PGN]

🔥 Surveillance Nation

"monty solomon" <monty@roscom.com>
Wed, 19 Mar 2003 17:30:58 -0500

Surveillance Nation [excerpt for RISKS]
Dan Farmer & Charles C. Mann, MIT *Technology Review*, cover story, Apr 2003

Webcams, tracking devices, and interlinked databases are leading to the elimination of unmonitored public space. Are we prepared for the consequences of the intelligence-gathering network we're unintentionally building?

Route 9 is an old two-lane highway that cuts across Massachusetts from Boston in the east to Pittsfield in the west. Near the small city of Northampton, the highway crosses the wide Connecticut River.

The Calvin

Coolidge Memorial Bridge, named after the president who once served as Northampton's mayor, is a major regional traffic link. When the state began a long-delayed and still-ongoing reconstruction of the bridge in the summer of 2001, traffic jams stretched for kilometers into the bucolic New England countryside.

In a project aimed at alleviating drivers' frustration, the University of Massachusetts Transportation Center, located in nearby Amherst, installed eight shoe-size digital surveillance cameras along the roads leading to the bridge. Six are mounted on utility poles and the roofs of local businesses. Made by Axis Communications in Sweden, they are connected to dial-up modems and transmit images of the roadway before them to a Web page, which commuters can check for congestion before tackling the road. According to Dan Dulaski, the system's technical manager, running the entire webcam system—power, phone, and Internet fees—costs just \$600 a month.

The other two cameras in the Coolidge Bridge project are a little less routine. Built by Computer Recognition Systems in Wokingham, England, with high-quality lenses and fast shutter speeds (1/10,000 second), they are designed to photograph every car and truck that passes by. Located eight kilometers apart, at the ends of the zone of maximum traffic congestion, the two cameras send vehicle images to attached computers, which use special character-recognition software to decipher vehicle license plates. The

license data go to a server at the company's U.S. office in Cambridge, MA, about 130 kilometers away. As each license plate passes the second camera, the server ascertains the time difference between the two readings. The average of the travel durations of all successfully matched vehicles defines the likely travel time for crossing the bridge at any given moment, and that information is posted on the traffic watch Web page.

To local residents, the traffic data are helpful, even vital: police use the information to plan emergency routes. But as the computers calculate traffic flow, they are also making a record of all cars that cross the bridge-when they do so, their average speed, and (depending on lighting and weather conditions) how many people are in each car.

<http://www.technologyreview.com/articles/farmer0403.asp>

U.S. lifts FBI criminal database checks

Peets <phobos@pobox.com>

Wed, 26 Mar 2003 18:15:30 +1100 (EST)

The Justice Department has lifted a requirement that is supposed to ensure the accuracy and timeliness of information about criminals and crime victims before it is added to the National Crime Information Center database, which includes data about terrorists, fugitives, warrants, people missing, gang members, and stolen vehicles, guns, and boats.

Records are queried increasingly by the nation's law enforcement agencies to help decide whether to monitor, detain or arrest someone. The records are [supposedly] inaccessible to the public, and police have been prosecuted in U.S. courts for misusing the system to find, for example, personal information about girlfriends or former spouses. [RISKS has noted at least two such cases resulting in deaths of the identified persons.]

Officials said the change, which immediately drew criticism from civil-liberties advocates, is necessary to ensure investigators have access to information that can't be confirmed but could take on new significance later, FBI spokesman Paul Bresson said. [...]

Critics have noted complaints for years about wrong information in the computer files that disrupted the lives of innocent citizens, and the FBI has acknowledged problems. In one case, a Phoenix resident was arrested for minor traffic violations that had been quashed weeks earlier; in another, a civilian was misidentified as a Navy deserter.

[Source: Ted Bridis, AP, 25 Mar 2003; PGN-ed]

http://news.yahoo.com/news?tmpl=story2&cid=542&u=/ap/20030325/ap_on_go_ca_st_pe/fbi_database_4&printer=1

✶ Text message disables Siemens mobile phones

"Derek K. Miller" <dkmiller@pobox.com>

Wed, 19 Mar 2003 10:15:19 -0800

MacInTouch.com relays a CNET News.com report by Ben Charny that a particular text message can disable cell phones manufactured by Siemens. The e-mails contain a single word, taken from the phone's language menu, surrounded by quote marks and preceded by an asterisk, such as "*English" or "*Deutsch", Siemens said. Opening the short-text message on a Siemens 35-series cell completely disables it [according to Siemens spokesman Jacob Rice]. Siemens 45-series phones are less affected and can be resuscitated after about two minutes of work. Both phones are sold only in Europe. The phones are not the victim of a denial of service attack, as suggested by some participating in an e-mail string on Bugtraq, a popular security e-mail list. "It's just not possible," Rice said. [Source: news.com, 18 Mar 2003]

<http://news.com.com/2100-1039-993197.html?tag=macintouch>

Derek K. Miller dkmiller@pobox.com <http://www.penmachine.com>
Penmachine Media Company, Vancouver, Canada

Wireless mushrooms

"brian-h seborg" <brian.seborg@telispark.com>

Thu, 20 Mar 2003 14:52:47 -0500

Many articles have covered wireless security issues from a technical perspective including the weaknesses in WEP, the fixes to WEP (fast-packet keying), and recommendations for securing a wireless network (802.1x,

suppress SSID broadcast, etc.), and I suspect that we in the technical community have a pretty clear understanding that tried and true network security solutions like SSL, SSH, firewalls, IPSec, two-factor authentication, etc. can be brought to bear to secure wireless networks in the same way we have used them to secure Internet and dial-up connections for years. The question is, do non-technical users have any knowledge of these things? My own experience is that the answer is "no."

ISPs, especially those offering DSL and high-speed cable modems aren't doing much if anything to make up for this deficit even though they are now delivering wireless routers to customer's homes. I have noticed that in the last month three more access points have popped up in my neighborhood. Of the five I can see, only one has WEP turned on and all are broadcasting their SSIDs (making them visible to even a novice). As I drive around in my car, I can easily connect to four of these access points. Further, when I checked to see if I can connect to the default administrative port, I can do so on all but the WEP protected one, and on three, I see they have not reset the default admin password, meaning I could, if I were a bad guy, reconfigure their router either rendering it useless (until they re-initialize it), or opening it to the Internet.

The fact that insecure access points are springing up like mushrooms makes it likely that we will begin to see a rash of hacked home users unless the high-speed Internet providers wake up and begin providing guidance to their customers about how to properly secure their wireless routers. In the case

where Internet providers are supplying the wireless gear, it would seem prudent that they would supply each device with a default safe configuration (random SSID, SSID broadcast suppressed, random admin username, random admin password, etc.). Unfortunately, like usual, appropriate measures are unlikely to be taken until security breaches begin to get noticed and customers begin to complain. In the meantime, as good neighbors, we might consider performing a high-tech neighborhood watch informing neighbors that their home networks are insecure. :-)

✶ Failure of aircraft electronic displays at a critical moment

"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>

Thu, 20 Mar 2003 08:52:17 +0100

David Learmount reports in Flight International, 11-17 Mar 2003, p12, on the loss of attitude information on the electronic attitude direction indicators (EADI) in a temporary loss-of-control incident due to icing with an Embraer Brasilia commuter turboprop operated by Comair.

The incident happened on 19 Mar 2001, and was investigated by the US National Transportation Safety Board. I have been unable to reach the FAA Incident Database to obtain the original documents (it refuses my connection).

The aircraft was cruising at 17,000 ft when it encountered icing conditions. It oscillated violently in roll (110 degrees left, 130 degrees

right, then a 360 degree roll to the right -yes, that's a full rotation) and pitched 60 degrees nose down. During this manoeuvre, the EADIs, which present crucial information to the pilots, "blacked out". The attitude indicator gives perhaps the most crucial control information available to pilots in instrument flight conditions. They recovered at 10,000 ft altitude when the aircraft emerged into visual flight conditions below the cloud. They pulled 3.6g to recover from the descent, itself a hairy manoeuvre.

"In subsequent test of the EADIs according to the production test requirements (PTR), the first officer's display was found to have an intermittent rate failure. However, the PTR does not test the equipment against its specified maximum performance in roll and pitch rate, not reacting in the icing incident until almost all the violent roll oscillations had occurred."

"The NTSB reports that the EADIs blacked out well before the specified performance limits had been reached, and benchtests in the performance area between the standard PTR criteria and specified performance limits caused both instruments to malfunction."

The NTSB apparently suggests that all Rockwell-Collins AHC-85 EADIs have been inadequately tested following manufacture and after maintenance. Rockwell-Collins apparently says that it did not carry out tests beyond PTR, and that the unit's performance at limits could be inferred from the results of the tests to PTR.

One cannot, and should not, conclude, however, that use of these electronic devices has led to new types of failures. Traditional mechanical gyroscopes would likely have tumbled in these manoeuvres, and the pilots would have thus been no better off. The issue that this incident highlights concerns the discrepancy between expected performance (represented by the PTRs and the "limits") and actual performance. This is a specification and testing issue.

Peter Ladkin, University of Bielefeld, Germany, <http://www.rvs.uni-bielefeld.de>

✶ A320 incident partly due to computer failure

"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>
Thu, 20 Mar 2003 18:03:17 +0100

John Sampson pointed out to me a computer-related incident to an A320.

On 21 May 1998, a Leisure International Airways A320 overran the runway at Ibiza Airport in the Balearic Islands. The damage was minor (broken nosewheel and consequent underbelly damage, dirt and stones ingestion in the engines, etc), and there were no serious injuries, so the incident probably does not rate as an accident.

The accident report is not long and a PDF version may be found at http://www.mfom.es/ciaiac/publicaciones/informes/1998/1998_019_A.pdf

Braking on landing is normally automatic, controlled by the Brake and Steering Control Unit (BCSU) computer. The BCSU is selected "on" during approach, by pressing the "A/SKID & N/W STRG" (Antiskid and nosewheel steering) button on the front panel in the cockpit. The BCSU has two identical channels, active ("hot") and standby, and there is a command (COM) and monitor (MON) function of the BCSU. MON checks COM for agreement before output is sent. Upon detection of a disagreement, a "disagree" condition is logged in the BCSU as well as sent to the Centralised Fault Data Interface Unit (CFDIU).

Suppose a fault develops and is detected in the hot channel. If hot and standby channels are both functioning, the system then transfers control to standby, which becomes hot and operates non-redundantly (that is, the faulty channel remains permanently cold). If standby is cold, hot remains active, control is not transferred, and one lives with whatever functions are still provided by the faulty hot channel.

The BCSU performs a functional test on selection of Landing Gear Down, opening the Normal Selector Valve, which allows pressure from the Green hydraulic system to reach the four servo valves of the Normal system (Normal Servo Valves, NSVs). The BCSU then sends current momentarily to the NSVs and monitors the pressure rise. It then closes the NSVs, closes Normal Selector Valve, and then opens the NSVs again to release the pressure. This will

have happened on the incident flight, says the report.

If the Normal braking system is inoperative, Alternate braking is made available by a spring-biased changeover valve (Automatic Selector Valve) which allows pressure from the Yellow hydraulic system to the Alternate braking system. Alternate braking is achieved through foot pedal pressure, transmitted hydraulically along a low-pressure line and ported through a Brake Dual Distribution Valve (BDDV) and a Dual Shuttle Valve to the Alternate servos on the brakes (these are separate devices from the NSVs). Antiskid is controlled by the BCSU, if still operative.

There is also a Parking Brake, operating off the Yellow system, backed up by a Brake Accumulator. Operating the Parking Brake handle applies unmodulated Yellow system hydraulic pressure (but reduced) to the brakes via the Parking Brake Valve.

Or so it all says here.

One problem is as follows. The status of the BCSU switch is sampled every 20 msec asynchronously by the COM and MON functions. It is possible that a short switch operation, from 20 ms to 50 ms, could be detected by one function and not by the other, causing a "disagree" fault in one, or indeed in both, channels of the BCSU. The analysis concludes that this indeed happened. The crew saw the "BRAKES BSCU Ch 2 FAULT" message on the Electronic Centralised Aircraft Monitoring (ECAM) display on selection of the BCSU. The message is listed in the Operating Manual as for

"Crew

Awareness" and there is no corresponding procedure. It turns out that the crew could have reset the BCSU but this info is not in the Abnormal and Emergency Procedures section of the Ops Manual, but in the Supplementary Techniques section, where it commences with the conditional "In case of braking /steering difficulty..." which they did not have because they were still in the air.

What will have then happened is that the hot channel, Channel 2, will have relinquished control to the standby, Channel 1, which will have logged the same fault, but cannot relinquish control since it is operating without a standby. On sensing touchdown ("Weight on Wheels"), four seconds after the spoiler deployment signal, the Autobrake function of the BCSU calls the command function to apply current to open the Normal Selector Valve. The COM/MON disagreement fault becomes a failure; the Normal Selector Valve is not opened, the Autobrake function is lost and the Normal braking system is left inoperative. This is recorded in the CFDIU as a failure in the NSVs (although the actual failure was upstream), which is sent to the ECAM as a "BRAKES AUTO BRK FAULT" message, which is inhibited from display during landing until engine shut down, but is recorded for post-flight replay. So the crew never saw it.

The Alternate system was inhibited due to moisture contamination of the BDDV, which it was presumed had turned to ice during flight and inhibited

operation of the BDDV. This course of events was confirmed by subsequent testing.

In principle, the crew could have used the parking brake, but they had not been so trained. It says in the operating manual that operating the parking brake deactivates the other braking systems.

At the end of the overrun area, there is a sea wall and the Mediterranean Ocean. Rather than risk taking a swim, the captain swerved the aircraft from side to side to lose momentum through scrubbing the tires, and then turned it finally 90 degrees away and bumped over the grass and into a low bank "to remain within the aerodrome boundary". The report describes the ride thereto as "quite rough".

BCSU software Release 7 was on board; Release 8 provides a fix for the sensing discrepancy condition involved in this incident; Release 9 was released after in-service experience with Release 8. I don't know what release is current.

Peter Ladkin, University of Bielefeld, Germany <http://www.rvs.uni-bielefeld.de>

✶ Paper is good

David Magda <dmagda+risks@magda.ca>
Sun, 23 Mar 2003 12:55:28 -0500

As we all (should) know, paper is still a useful thing to have around.

A weblog entry from [1]:

--- entry ---

Sat, 22 Mar 2003

Books in Print Wouldn't Fit

An odd thing happened on my way to buy a book at my local Barnes and Noble.

[Yes, yes, before you go and point it out, any story that starts out this

way is almost certainly my fault.]

Me: Can you tell me who the author of _____ is?

Retailer: I can't.

Me: Well, can you look it up?

Retailer: I can't. Our computers are down.

Me: Ah. Well, can I take a gander at your Books in Print.

Retailer: [Smirks] We don't have a list of all the books in print.

We wouldn't be able to fit it in the store.

Me: In fact you would. We had these great big volumes and then later

microfiche when I worked in a bookstore a number of years back.

Retailer: Do you know how many books that would be?

Me: Lots, I do believe you. But the fact remains that Books in Print

is indeed a real thing.

Retailer: Well, we don't have it. We have computers instead.

Me: Apparently not.

[Only ever so slightly paraphrased.]

--- entry ---

Book in Print(tm) can be found online at [2]: assuming that your computer is up, the 'Net is working, and their computer is up. :

> You

need an account to search their online catalogue. A paper version is

described at [3].

- [1] http://www.raelity.org/archives/society/literature/books_in_print_wouldnt_fit.html
- [2] <http://www.booksinprint.com/bip/>
- [3] <http://www.bowker.com/bowkerweb/catalog2001/bibtoc.htm>

David Magda <dmagda at ee.ryerson.ca>

... Because the innovator has for enemies all those who have done well under the old conditions, and lukewarm defenders in those who may do well under the new. -- Niccolo Machiavelli, *The Prince*, Chapter VI

FTC's National Telemarketing "Do Not Call" Web Site to Launch 1 Jul

CDT Info <info@cdt.org>

Wed, 26 Mar 2003 15:06:50 -0500

[via Monty Solomon]

The Federal Trade Commission has announced that the Web site allowing consumers to put their telephone numbers on the national registry to stop telemarketing calls will launch in July. The FTC will also have a toll free number to call. The FTC expects overwhelming demand for the project and is therefore rolling out the toll free number beginning on the west coast and heading east throughout the summer. March 26, 2003

The FTC The National "Do Not Call" Registry Page

<http://www.ftc.gov/bcp/conline/edcams/donotcall/index.html>

Comments of CDT and others to FTC supporting "Do Not Call" list [pdf] March 28, 2002

<http://www.cdt.org/privacy/020328cpg-dnc-comments.pdf>

CDT comments to FCC on "Do Not Call" December 9, 2002

<http://www.cdt.org/privacy/021209cdt.shtml>

<http://www.cdt.org/mailman/listinfo/cdt-announcements>

Transient Microsoft Passport security vulnerability

"James Van Bokkelen" <jbvb@sandstorm.net>

Wed, 19 Mar 2003 16:05:18 -0500

When a laptop arrived last week with a sacrificial Windows XP Home Edition installed on it, we combined curiosity with a testing opportunity, and analyzed its network traffic with our NetIntercept tool. After using UDP-based protocols to locate resources, and HTTP and HTTP over SSL to register itself, the WinXP installer asked if we wanted to create a .NET Passport account. We agreed. After an initial exchange with host nexus.passport.com using HTTP over SSL, subsequent HTTP connections used normal HTTP on port 80.

We were quite surprised by several POST commands to register.msna.passport.net. Each contained plaintext answers to the previous screen's questions. All the critical data necessary to hijack the .NET passport was exposed: name, birthday, ZIP, gender, occupation, password and secret question/answer. A more detailed analysis can be found at

<http://www.sandstorm.net/passport>

This took place on the morning of 14 Mar 2003. Microsoft was informed as soon as we made our way through the obfuscation protecting the proper channels, and they assured us the problem was being worked on. Testing on 17 Mar led us to believe it was fixed, and Microsoft confirmed this later in the day. They told us the problem had been introduced as part of routine web site maintenance earlier in the week. Because it didn't involve customer software, they didn't plan to issue a security bulletin.

The risks associated with maintaining systems are well known; I expect an enormous number of people have studied that particular set of transactions since the Passport roll-out. However, any others who looked during the period of vulnerability apparently didn't inform Microsoft. Presumably we won't hear more unless a rash of identity theft generates publicity.

Although I've been involved with the Internet for years, I had avoided using my credit card over the net until this month. Given current tools, I'll feel compelled to read the page source before I do so again.

⚡ Re: Traffic lights don't work in the snow ([RISKS-22.62](#))

"Ryan O'Connell" <ryan-risks@complicity.co.uk>
Tue, 11 Mar 2003 10:02:46 +0000 (GMT Standard Time)

This is not a new problem for anyone used to riding a small (125cc - 7.6

cubic inches I believe is the US measurement) motorbike. Many small sports motorbikes are made almost entirely of alloy to reduce their weight. (The Aprillia RS125 is an example) Sometimes, there's not enough metal in the bike to trigger these sensors - leaving you sitting at the lights wondering what to do next. On many roads you can't turn round so you just have to risk running the red light.

Fortunately, when this happens it's usually late at night so there's no other traffic about to trigger the lights and therefor no other traffic that can hit you.

On a busy road, the risks are obvious. You have no choice but to attempt to join a potentially busy road by going through a red light or ride on the pavement to a safe spot to rejoin traffic. (I usually chose the latter option.)

✶ Re: Beware the spelling checker (NewsScan, [RISKS-22.64](#))

Crispin Cowan <crispin@wirex.com>
Tue, 18 Mar 2003 17:05:51 -0800

> ... However, using the software, the two groups made about the same number
> of errors -- 16 vs 17.

What this experiment does not account for is to compare the 16 or 17 errors in a document assisted by the spelling checker vs. the error

rate in documents that are never proof read at all because the author could not be bothered.

Crispin Cowan, Chief Scientist, WireX <http://wirex.com/~crispin/>
HP/Trend Immunix <http://h18000.www1.hp.com/products/servers/solutions/iis/>



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 66

Tuesday 1 April 2003

Contents

- [The Security Flag in the IPv4 Header](#)
[Steve Bellovin](#)
- [The Angelic Bit vs the Evil Bit](#)
[Drew Dean](#)
- [Alternative electronic recycling](#)
[PGN](#)
- ['Reverse production' system recycles all](#)
[NewsScan](#)
- [Use a Firewall, Go to Jail](#)
[Ed Felten via Monty Solomon](#)
- [Re: Use a Firewall, Go to Jail](#)
[Steven M. Bellovin](#)
- [State Super-DMCA too true](#)
[William Allen Simpson](#)
- [Voting machine article in *The Washington Post* by Dan Keating](#)
[James Paul](#)
- [Internet vs. the recording industry](#)
[NewsScan](#)
- [To unlock safe... please endanger your financial future](#)
[Jack Burke](#)

- [Re: Friendly fire](#)
[Hugo Tyson](#)
 - [Aircraft software maintenance](#)
[Martyn Thomas](#)
 - [Risks in reading RISKS links](#)
[Doug Sibley](#)
 - [Re: Beware the spelling checker](#)
[Bodo Moeller](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ The Security Flag in the IPv4 Header

<Peter Neumann <Neumann@CSL.sri.com>>

1 April 2003

Steve Bellovin's RFC 3514 (released today) assigns a meaning to the IPv4 packet header's last currently unused bit, which can be thought of as a Security Flag. Benign packets have this bit set to 0; those that are used for an attack will have the bit set to 1. Correct functioning of security mechanisms depends critically on the bit being set properly. If faulty components do not set the bit to 1 when appropriate, firewalls will not be able to do their jobs properly. Similarly, if the bit is set to 1 when it shouldn't be, a denial of service condition may occur.

Following is a summary of the assigned values in the RFC:

0x0 If the bit is set to 0, the packet has no evil intent. Hosts, network elements, etc., SHOULD assume that the packet is harmless, and SHOULD NOT take any defensive measures. (We note

that this part of the spec is already implemented by many common desktop operating systems.)

0x1 If the bit is set to 1, the packet has evil intent. Secure

systems SHOULD try to defend themselves against such packets.

Insecure systems MAY chose to crash, be penetrated, etc.

It is well worth your reading the full RFC, which is now available:

<ftp://ftp.rfc-editor.org/in-notes/rfc3514.txt>

[See the IETF Web site for the full set of RFCs, for those of you not used

to reading them. It is an extraordinary view of the history of the

ARPAnet and Internet:

<http://ftp.rfc-editor.org>

PGN]

⚡ The Angelic Bit vs the Evil Bit

<Drew Dean <ddean@csl.sri.com>>

Tue, 1 Apr 2003 10:00:01 +1000

Steve Bellovin's proposed RFC 3514 finds a very constructive use for the

last unused bit in the IPv4 header. In his proposal, the unused bit is

sometimes affectionately referred to as the "evil" bit, although that naming

convention reflects a fundamentally *pessimistic* world view.

We prefer an

optimistic world view, and therefore propose that this last bit should be

used for the "angelic" bit. Our proposed semantics for the

angelic bit are
as follows:

0x1 The angelic bit is set. All routers, firewalls, switches, and any other network devices MUST forward this packet to its indicated destination. This packet MUST NOT have any undesirable effect on any network device. Anyone who improperly sets the angelic bit on any packet SHALL be subject to divine retribution. Civil authorities MAY subject the perpetrator to any punishment provided for in applicable law.

0x0 The angelic bit is reset. All routers, firewalls, switches, and other network devices MAY filter this packet according to any policy they deem fit. This packet MAY have undesirable effects if forwarded. The sender of the packet SHALL NOT be subject to divine retribution in case of undesirable effects. Civil authorities MAY subject the perpetrator to punishment provided for in applicable law.

NB: The angelic bit may have miraculous properties in face of network links severed by backhoes; however, this SHALL NOT relieve the router of its responsibilities.

Yours for a more genteel Internet, Drew Dean

[Note added 1 Oct 2003 by PGN in RISKS archive copy:

From Peter Gutmann's "X.509 Style Guide"

<http://www.cs.auckland.ac.nz/~pgut001/pubs/x509guide.txt>

One might as well add a "crimeFree" (CF) bit with usage

specified as 'The crimeFree bit is asserted when subject public key is used to verify digital signatures for transactions that are not a perpetration of fraud or other illegal activities'

-- Tony Bartoletti on ietf-pkix

My apologies to Tony for not giving him proper attribution.... Drew]

[Alternative electronic recycling \(Re: Reverse production, R-22.66\)](#)

<Peter Neumann <Neumann@CSL.sri.com>>

1 April 2003

Perhaps inspired by the Georgia Tech 'reverse production' recycling scheme for computer hardware [see the FOLLOWING item], computer scientists have discovered a way to recycle previously used computer cycles and previously generated data. The trick is first to compress newly written programs using an approach similar to Kolomogorov Complexity analysis, and then map the results into callable elements of old programs that can directly give the desired results in return. Research is underway that would even enable the used cycles of old programs written in archaic languages such as COBOL and FORTRAN to be recycled in this way. Optimizing compilers are already being developed to make this practical, incorporating formal methods (e.g., theorem proving and model checking) to ensure that only provably correct program elements are allowed. In addition, some artificial

intelligence

groups reportedly believe that automatic program synthesis techniques could be used to avoid writing the new programs altogether, thus surmounting the existing limitations of bad software engineering while still obtaining highly efficient programs.

It is estimated that this approach could substantially reduce the burgeoning need for more cycles and new storage capacity. When applied to Windows operating systems, initial experiments show that this could result in at least a 70% reduction in program size and execution time.

Purveyors of electronic voting machines are intrigued by the possibility of reusing the results of previous elections, with suitable parametric transformations.

However, several computer vendors are objecting on the grounds that widespread use of this technique could detrimentally result in a "compression depression" trickle-down effect of decreased revenue that could more than completely negate the beneficial hardware demands that result from steadily increasing bloatware and the constant need for upgrades. In addition, programmers' unions are contemplating strikes if this technique becomes widely adopted.

The word 'reverse' also brings to mind some research results on programs that can be run backwards (for example, implementing information lossless algorithms that work forwards and backwards, and also environments in which 'undo' operations can be successfully executed). Use of such programs could result in saving a further factor of two.

A previously proposed alternative approach of creating a very large number of randomly generated compressed programs and then finding the one that works best for the given application has unfortunately been temporarily abandoned as unworkable, pending further research. That approach had been conceived in response to the somewhat obscure but truly classical 1961 paper, subsequently reprinted as ``The Chaostron: An Important Advance in Learning Machines'', J.B. Cadwallader-Cohen, W.W. Zysiczk, and R.B. Donnelly, *Communications of the ACM*, April 1984, pages 356--357).

✶'Reverse production' system recycles all

<"NewsScan" <newsscan@newsscan.com>>

Wed, 05 Mar 2003 09:25:28 -0700

A study underway at Georgia Tech could offer a model for responsible recycling of electronic waste. Researchers have developed a "reverse production" system that enables every raw material contained in e-waste -- metals such as lead, copper, aluminum and gold, as well as plastics, glass and wire -- to be recovered and reused. Scientists say such "closed loop" manufacturing offers a win-win situation for manufacturers and consumers, and the project is generating buzz abroad, with officials in Taiwan and Belgium expressing interest in the system. Key to the process is chemical engineer Matthew Realff's design for a means to separate metals,

as well as different qualities of plastics from crushed, ground-up components. From this work, new industries could be created to recover value not only from e-waste, but also from automobiles and other durable goods, says Realff.

(*Science Daily*, 4 Mar 2003; NewsScan Daily, 5 March 2003)

<http://www.sciencedaily.com/releases/2003/03/030304073140.htm>

Use a Firewall, Go to Jail

<Monty Solomon <monty@roscom.com>>

Fri, 28 Mar 2003 15:36:25 -0500

<http://www.freedom-to-tinker.com/archives/000336.html>

March 26, 2003

Ed Felten, Use a Firewall, Go to Jail

The states of Massachusetts and Texas are preparing to consider bills that apparently are intended to extend the national Digital Millennium Copyright Act. (TX bill; MA bill) The bills are obviously related to each other somehow, since they are textually similar.

Here is one example of the far-reaching harmful effects of these bills. Both bills would flatly ban the possession, sale, or use of technologies that "conceal from a communication service provider ... the existence or place of origin or destination of any communication". Your ISP is a communication service provider, so anything that concealed the origin or destination of

any communication from your ISP would be illegal -- with no exceptions.

If you send or receive your e-mail via an encrypted connection, you're in violation, because the "To" and "From" lines of the e-mails are concealed from your ISP by encryption. (The encryption conceals the destinations of outgoing messages, and the sources of incoming messages.)

Worse yet, Network Address Translation (NAT), a technology widely used for enterprise security, operates by translating the "from" and "to" fields of Internet packets, thereby concealing the source or destination of each packet, and hence violating these bills. Most security "firewalls" use NAT, so if you use a firewall, you're in violation.

If you have a home DSL router, or if you use the "Internet Connection Sharing" feature of your favorite operating system product, you're in violation because these connection sharing technologies use NAT. Most operating system products (including every version of Windows introduced in the last five years, and virtually all versions of Linux) would also apparently be banned, because they support connection sharing via NAT.

And this is just one example of the problems with these bills. Yikes.

UPDATE (6:35 PM): It's worse than I thought. Similar bills are on the table in South Carolina, Florida, Georgia, Alaska, Tennessee, and Colorado.

UPDATE (March 28, 9:00 AM): Clarified the paragraph above about

encrypted
e-mail, to eliminate an ambiguity.

Posted by Edward W. Felten

[Moderator's note: This item is NO JOKE, despite the date of this issue.

Check out the thread that is occurring subsequent to Ed Felten's message:

<http://www.freedom-to-tinker.com/archives/000336.html>

as well as the next two messages in this issue, from Steve Bellovin and

William Allen Simpson. PGN]

✶ Re: Use a Firewall, Go to Jail

<"Steven M. Bellovin" <smb@research.att.com>>

Fri, 28 Mar 2003 19:08:42 -0500

After reading the full text of the Texas bill

(<http://www.capitol.state.tx.us/data/docmodel/78r/billtext/pdf/HB02121I.PDF>),

I think it may be even worse than Felten portrays it.

First, a number of people have claimed that the bill isn't a problem, since it only applies if you intend to harm or defraud an ISP. I don't think that that's the case.

Section 2 of the bill, which does contain the phrase "with the intent to harm or defraud a communication service", bars theft of service. (I'm speaking loosely here; read it for yourself.)

Section 4 also contains that phrase; it bars possession of devices for

defrauding providers. (The language is very broad, and seems to bar possession even a computer or modem if you have evil intent.)

The ban on concealing origin or destination is in Section 6. That section does **not** have the "intent to harm" phrase. Given that the bill is amending three consecutive sections of the state penal code (31.12, 31.13, and 31.14), and given that the first two sections have that language but the third doesn't, it's hard for me to conclude that evil intent is required by the proposed statute.

But it's worse than that: the bill bars concealment of "existence or place of origin or destination of any communication" from "any lawful authority". In other words, it would appear to outlaw many forms of cryptography or steganography, or anonymous remailers. (As an aside, I would note that the constitutional justification for easy law enforcement access to source and destination address information via the pen register statute is flimsy at best -- see my analysis at <http://www.research.att.com/~smb/talks/Wiretaps/index.htm>)

Even Web proxy servers and the Ethernet connectivity from many hotels would be covered by this bill -- they obscure the origin, too.

What's unclear to me is who is behind this. Felten implies it's content providers trying for a state-level DMCA; I think it's broadband ISPs who are afraid of 802.11 hotspots. In fact, if the "intent to cause harm" phrase were added to that section, it would clearly criminalize behavior that some ISPs are trying to ban today via their terms of service.

Steve Bellovin, <http://www.research.att.com/~smb> <http://www.wilyhacker.com>

State Super-DMCA too true (from NANOG)

<William Allen Simpson <wsimpson@greendragon.com>>

Sat, 29 Mar 2003 15:53:32 -0500

[Courtesy of Steve Bellovin. PGN]

Declan McCullagh sent out an e-mail this morning, referencing his full report at:

<http://news.com.com/2100-1028-994667.html>

I was shocked to see that Michigan has **already** passed such a law!

(Also Virginia, Delaware, and Illinois.)

I've found the new law(s), and they basically outlaw my living in Michigan starting March 31st (this Monday, two days from now):

<http://www.michiganlegislature.org/printDocument.asp?objName=mcl-750-219a-amended&version=txt>

<http://www.michiganlegislature.org/printDocument.asp?objName=mcl-750-540c-amended&version=txt>

The Bill analysis basically quotes the MPAA website!

<http://michiganlegislature.org/documents/2001-2002/billanalysis/house/htm/2001-HLA-6079-b.htm>

It outlaws all encryption, and all remailers.

It outlaws connecting any device "without the express authority of the telecommunications service provider". No NATs. No wireless.

(Some DSL/cable companies try to charge per machine, and record the machine address of the devices connected.)

It outlaws configuring your ISDN to be a voice device, and then sending data over the device.

(Most folks around here are willing to settle for 56Kbps + 56Kbps -- fixed fee -- instead of 64Kbps + 64Kbps -- per minute.)

It outlaws configuring a wire pair purchased as a burglar alarm circuit, and then using it as DSL.

It outlaws using Linux/*BSD for reading DVDs and a host of other things.

Also, "reprogramming" a device (and software and computer chips are explicitly included) "that is capable of facilitating the interception, transmission, retransmission, decryption, acquisition, or reception of any telecommunications, transmissions, signals, or services" would seem to prohibit mod'ing of M\$ Xboxen.

Heck, it is possible to read this Act to prohibit changing your operating system from M\$ to Linux.

This was passed in a lame duck session (December 11, 2002) as part of a big omnibus crime act that covered everything from "adulteration of butter and cream", to "trick or acrobatic flying" to "false weights and measures", mostly increasing fines and/or jail for existing offenses. Michigan is a leader in overcrowding its prisons.

There was other lame duck legislation passed, before a new

Governor took
office, almost all of it bad for civil liberties!

William Allen Simpson

🔥 Voting machine article in *The Washington Post* by Dan Keating

<james.paul@mail.house.gov>

Fri, 28 Mar 2003 01:27:21 -0500 (EST)

As election officials rush to spend billions to update the country's voting machines with electronic systems, computer scientists are mounting a challenge to the new devices, saying they are less reliable and less secure from fraud than the equipment they are replacing. Prompted by the demands of state and federal election reforms, officials in Maryland, Georgia, Florida and Texas installed the high-tech voting systems last fall. Officials in those states, and other proponents of electronic voting, said the computer scientists' concerns are far-fetched. [...]

David Dill, the Stanford University professor of computer science who launched the petition drive, said, "What people have learned repeatedly, the hard way, is that the prudent practice -- if you want to escape with your data intact -- is what other people would perceive as paranoia." Other computer scientists, including Rebecca Mercuri of Bryn Mawr College, say that problems are so likely that they are virtually guaranteed to occur -- and already have.

[Source: Dan Keating: New Voting Systems Assailed, *The Washington Post*,

27 Mar 2003; PGN-ed]

<http://www.washingtonpost.com/wp-dyn/articles/A39241-2003Mar27.html>

See David Dill's petition at

<http://verify.stanford.edu/evote.html>

PGN]

Internet vs. the recording industry

<"NewsScan" <newsscan@newsscan.com>>

Fri, 28 Mar 2003 10:47:35 -0700

Media analyst Eric Garland of Big Champagne has told California lawmakers

that the growth of music file-sharing on the Internet is "fundamentally

unstoppable," because 61 million Americans and millions more worldwide are

already downloading music and only 9% of them think they're doing something

wrong. "We see only one trend. More people are downloading more copyrighted

material." Garland's advice for the recording industry is to embrace digital

distribution rather than institute lawsuits or education campaigns, but such

advice is not well-received by industry executives, who are routinely urged

by Internet enthusiasts to accommodate to technological realities. Phil

Corwin, a lobbyist for Internet music service Kazaa, told the same group of

state legislators: "The record business, in the digital revolution, has been

a day late and a dollar short." [A dollar may not be the final figure.] The

fight goes on. [AP/*San Jose Mercury News*, 28 Mar 2003;
NewsScan Daily, 28
March 2003]

<http://www.siliconvalley.com/mld/siliconvalley/5502291.htm>

⚡ To unlock safe... please endanger your financial future

<Jack Burke <jfb3@mindspring.com>>

Fri, 28 Mar 2003 16:41:25 -0500

A local (Atlanta, Georgia) radio station is running a contest (what else is new?) for callers to enter. (I won't mention B98.5's call letters to save them the embarrassment.) It's the same standard formula: when you hear a particular song, be the 42,828,210,193 listener to call in for "your chance to win." The grand prize is \$2 million.

The "gimmick" in this one is that the money is in a safe. To unlock the safe, a potential vict^H winner must give the DJ the 5 one-digit numbers in the combination--but not just any 5 numbers will do. Callers are asked for the last 5 digits of their social security number. (Presumably the station will require verification before actually paying out the "winnings.")

Did I mention that this was all done on the air? Can anyone guess how many people I've heard willingly gush out five-ninths of their SS number and first and last name on the air?

In 3 seconds or less, how many different things can you think of

for which
all or part of a social security number is used?

- Social security "benefits"
- credit applications
- credit reports
- PINs for telephone access to account information (banks, etc.)

Can anyone say: "shortcut to identity theft"? (Not as far-fetched as you might think. The first three digits are based on the state in which you apply for the number in the first place, which stands a reasonable chance of being where you were born. That's an easy topic for a conversation with someone who you "accidentally" meet.)

⚡ Re: Friendly fire (was: Patriot software again a concern?)

<Hugo Tyson <hmt@surfingsuggestion.co.uk>>

Fri, 28 Mar 2003 18:31:08 GMT

In [Risks Digest 22.65](#) PGN wrote:

> [Incidentally, NBC on 24 Mar 2003 had an item on self-inflicted
> damage, noting that in the Vietnam War, 24% of U.S. fatalities were
> due to friendly fire. I have heard reports that it was even higher
> in the first Gulf War. That is truly astounding! PGN]

Not sure whether it's a computer risk, but this is a social risk in terms of expectations about such things, due to the high-tech weapons now available to *some* armed forces: when one side has far better offensive weapons and

far better defensive weapons than the other, a consequence is that friendly-fire incidents will dominate the casualty list for the better-armed side, simply because the less-well-armed side won't be able to harm the better as much as FF can. The same applies to night-vision gear, intelligence, surveillance and all that.

For example:

Offensively, if only one side can see clearly at night, only that side will be able to hit things **at all** - even if they're not sure whose things.

Defensively, the flip-side: if only an Abrams round can kill an Abrams tank, then 100% of Abrams destroyed will be FF.

Not suggesting this is so across all encounters in the current war by any means, but in tank vs. tank, aircraft vs. ground vehicle, and aircraft vs. anti-aircraft/anti-missile I think it has the ring of truth.

✈ Aircraft software maintenance (Re: Ladkin, [RISKS-22.65](#))

<"Martyn Thomas" <martyn@thomas-associates.co.uk>>
Fri, 28 Mar 2003 18:18:24 -0000

In a recent posting on an A320 Airbus software fault that contributed to a loss of braking, Peter Ladkin wrote: "BCSU software Release 7 was on board; Release 8 provides a fix for the sensing discrepancy condition involved in this incident; Release 9 was released after in-service

experience with
Release 8."

Does this mean that a fault was introduced in Release 8 that was not found in testing/recertification but that showed up fairly quickly in operational use? If so, does this suggest that the process for introducing maintenance changes needs improvement?

I have never understood how changes to safety-related software can be introduced rapidly without the formal specifications and formally defined languages that might allow the maintenance group to be completely confident about the scope of the necessary reverification/revalidation. Can anyone explain? Or is there a process weakness here that will one day contribute to an accident?

✶ Risks in reading RISKS links

<Doug Sibley <sibley@acm.org>>
Fri, 28 Mar 2003 16:14:26 -0500 (EST)

With a referral from RISKS, an article by Dan Farmer, and the MIT name, I expected the link in [RISKS 22.65](#) (<http://www.technologyreview.com/articles/farmer0403.asp>) to be viewable without any significant risks (sorry for saying the word "risk" so many times).

Unfortunately, there were many. It requires registration (so I need to link

my e-mail address to the viewing of this article -- privacy invasion but whatever (it gives me the idea for a server where people could create temporary/throwaway receive-only e-mail accounts where messages would only be stored for a few hours for the only purpose of signing up at places like this -- although I can imagine it would violate the DMCA in some way).

Getting back to the risks: the form has one starred field for passwords instead of the usual two. I entered a username and then entered a password twice (as is normally required) and clicked submit. So I entered my password as my first name. Since the form required a postal code, etc. I had to re-fill-out the form. Given that they starred the password, one would expect that (a) the password would not be stored, and (b) that it would not be displayed. When you submit though, your password is e-mailed to you.

I would expect large institutions like MIT to have figured out passwords by now but my cellular provider also does not. Bell Mobility stores passwords online and there are two account preferences-type views, one has the password starred and the other unstarred (of course the password is kept in all-caps to make password guessing easier). In fact, when I was having problems a Bell Mobility representative e-mailed asking for my password (which I reported but never got back from). American Express limits passwords to 8 character alpha-numeric.

How long will it take for companies with reputation and value at

stake to
properly manage risks? Why is password security so poorly done
in practice
when it is such a well-studied problem?

✶ Re: Beware the spelling checker (Cowan, [RISKS-22.65](#))

<Bodo Moeller <moeller@cdc.informatik.tu-darmstadt.de>>

Mon, 31 Mar 2003 18:02:37 +0200 (MEST)

The interesting aspect about spilling chicken software is that
it helps you
make sure you keep only those errors that actually distort the
meaning.

Automatic correction is even more interesting in this respect.

True story: a German collection of law texts (from by a private
publisher)

consistently uses the word "Regenschutz" when it should say
"Regelsatz".

The latter roughly translates to "standard rate" (this is in
regulations
concerning public-welfare aid); the former means "rain
protection".

It was not problem to figure out what the text should have
said. The
problem was just that you are not supposed to laugh loudly in
public
libraries.

TU Darmstadt, Theoretische Informatik, Alexanderstr. 10, D-64283
Darmstadt

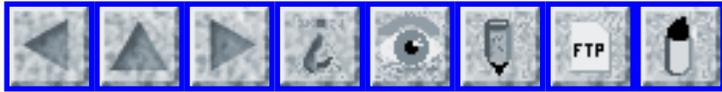
Tel. +49-6151-16-6628, Fax +49-6151-16-6036

[Better known perhaps is the word "Regenschirm" -- an
umbrella, or
literally, a screen against the rain -- which of course was

what was

needed for protection during the Reagan administration.

Danke! PGN]



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

[ACM](#) Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 67

Friday 4 April 2003

Contents

- [Rice cooker reprograms pacemaker?](#)
[Mark Batten-Carew](#)
- [eBay reacts to charges against its Paypal operation](#)
[NewsScan](#)
- [Pennsylvania won't identify sites blocked for child porn](#)
[Ted Bridis via Monty Solomon](#)
- [The Googlewashing of our language](#)
[Alpha Lau](#)
- [Is your television watching you?](#)
[Phillip Swann via Monty Solomon](#)
- [Website hoax on killer virus triggers Hong Kong panic](#)
[Monty Solomon](#)
- [Ellison predicts major shakeout in Silicon Valley](#)
[NewsScan](#)
- [Music piracy violations: \\$150K a song](#)
[NewsScan](#)
- [Streaming video: a patent on porn](#)
[Monty Solomon](#)
- [Laws make crypto and untraceable E-mail illegal?](#)
[Douglas W. Jones](#)

- [The reality behind these laws](#)
[Fred Cohen](#)
 - [State Super-DCMAs will be suicidal](#)
[David Harmon](#)
 - [Draft legislation on using crypto](#)
[Anick Jesdanun via Dave Farber to PGN](#)
 - [Re: Draft legislation on using crypto](#)
[David P. Reed](#)
 - [Patriot software again a concern?](#)
[Robert I. Eachus](#)
 - [Friendly Fire and the Perils of Statistical Reasoning](#)
[Thomas A. Russ](#)
 - [Re: Friendly fire](#)
[Anthony Youngman](#)
 - [NCIC: "Death by Oops?"](#)
[Lauren Weinstein](#)
 - [POW Social Security numbers revealed](#)
[Paul Hirose](#)
 - [Cell phones & 911 service](#)
[Jeremy Epstein](#)
 - [Possibly-wrong expectations about bouncing e-mail](#)
[Mark T.B. Carroll](#)
 - [Info on RISKS \(comp.risks\)](#)
-

🔥 Rice cooker reprograms pacemaker?

"Mark Batten-Carew" <markbc@paulmartin.ca>
Tue, 1 Apr 2003 12:56:24 -0500

This is an excerpt from a monthly newsletter that sends out interesting news items. I don't believe this is an April Fools' item, but then who knows? Mark Batten-Carew

HEARTBREAKING

A Japanese woman's automatic rice cooker changed the settings on her

pacemaker. Doctors doing a routine check up were baffled to find that the

hi tech pumping device they had implanted in the woman, 60, had been

remotely adjusted. They contacted the manufacturer, who visited her home

and found that a rogue rice cooker had somehow beamed signals to the

device. [Source: A&A Economic Digest - April 2003 Edition, <http://www.aacb.com/edigest/>, 1 April 2003]

[Quite plausible, in light of previous reported cases of electromagnetic

interference on pacemakers

--- from ACM Software Engineering Notes back issues:

* Arthritis-therapy microwaves set pacemaker to 214, killed patient (S 5 1)

* Retail-store anti-theft device reset pacemaker, man died (S 10 2, 11 1)

* Pacemaker locked up when being adjusted by doctor (S 11 1)

* Electrocauterizer disrupts pacemaker (S 20 1:20)

--- and from RISKS:

* Stores' shoplifting gates can set off pacemakers, defibrillator ([RISKS-20.05](#))

* Heart pacemaker and implantable cardioverter defibrillator recalls and alerts involve 520,000 devices (S 26 6:8, [RISKS-21.60](#))

PGN]

eBay reacts to charges against its Paypal operation

"NewsScan" <newsscan@newsscan.com>

Tue, 01 Apr 2003 10:43:01 -0700

Federal prosecutors in Maryland have accused PayPal, the

Internet payments
company acquired by eBay, of violating the Patriot Act by
facilitating
illegal gambling. The company disclosed the accusation in its
annual report
filed with the Securities and Exchange Commission; it says that
prosecutors
have offered a complete settlement of all possible claims and
notes that the
amount of its earnings from online gambling was less than what
prosecutors
asserted. [AP/*San Jose Mercury News*, 31 Mar 2003; NewsScan
Daily, 1 Apr
2003]

<http://www.siliconvalley.com/mld/siliconvalley/5525363.htm>

✶ Pennsylvania won't identify sites blocked for child porn (Ted Bridis)

Monty Solomon <monty@roscom.com>
Thu, 3 Apr 2003 22:09:01 -0500

Mike Fisher, Pennsylvania's attorney general, is citing laws
against
distributing child pornography in refusing to identify any of
hundreds of
Web sites his office has forced Internet providers to block
under a unique
state law that the Center for Democracy and Technology asserts
is blocking
Web surfers from accessing legitimate sites, but cannot prove
without access
to the list of blocked sites. Fisher's office said disclosing
the list of
blocked Web sites would itself be disseminating such
pornography, which is
illegal. [Source: Ted Bridis, AP Online, 3 Apr 2003; PGN-ed]
<http://finance.lycos.com/home/news/story.asp?story=33704697>

✶ The Googlewashing of our language

Alpha Lau <avlxyz@yahoo.com>

Thu, 3 Apr 2003 22:06:12 -0800 (PST)

Taken from Slashdot [1]:

"The Register[2] talks about how a term ("Second Superpower") coined by the anti-war culture suddenly got radically neutered and altered by a weblog[2] that a lot of people link to. Searching for the term on Google now brings up his blog and other people talking about his blog for the first several entries. Can Google's power to give information to the people be misused and perverted? This only took 42 days." First the widespread usage of "googling" to mean web searching, and now this.

The Register article [2] has the details and how powerful google can be.

[3] is the weblog that managed to saturate Google's PageRank.

I had a quick peek on AltaVista and voila, numerous other usages of the term "Second Superpower" [4].

The Risk? Blindy trusting Google and it's proprietary PageRank algorithm.

Worse yet, as Google gains users trust, it is very easy to trust Google alone.

- [1] <http://slashdot.org/article.pl?sid=03/04/03/2327239&mode=nested&tid=95>
 - [2] <http://www.theregister.co.uk/content/6/30087.html>
 - [3] <http://cyber.law.harvard.edu/people/jmoore/secondsuperpower.html>
 - [4] <http://www.altavista.com/web/results?q=Second+Superpower&kgs=0&kls=1&avkw=xytx>
-

✶ Is your television watching you? (Phillip Swann)

Monty Solomon <monty@roscom.com>

Tue, 1 Apr 2003 14:35:48 -0500

Could the federal government find out what you're watching on TV? Even if you're not the subject of a criminal investigation? If you're a satellite TV or TiVo owner, the answer is yes, according to legal experts and industry officials.

Under the USA Patriot Act, passed a month after the 9/11 terrorist attack, the feds can force a noncable TV operator to disclose every show you have watched. The government just has to say that the request is related to a terrorism investigation, said Jay Stanley, a technology expert for the American Civil Liberties Union.

Under Section 215 of the Act, you don't even have to be the target of the investigation. Plus, your TV provider is prohibited from informing you that the feds have requested your personal information. ...

Source: Phillip Swann, TVWeek.com

<http://www.tvweek.com/technology/030303isyourtv.html>

Website hoax on killer virus triggers Hong Kong panic

Monty Solomon <monty@roscom.com>

Tue, 1 Apr 2003 09:42:02 -0500

[Source: Tan Ee Lyn, Reuters, 1 Apr 2003; PGN-ed]

A teenager's Web Site hoax about the killer virus sweeping Hong Kong sparked panic food buying and hit financial markets on Tuesday, and the government said it was placing more than 200 people into isolation camps.

Indonesia, the world's fourth most populous nation, reported its first three suspected cases. One official said one of the patients had died but this could not be confirmed.

Severe Acute Respiratory Syndrome (SARS) has now affected almost 1,900 people in at least 12 countries, and 63 are known to have died.

In Hong Kong, where 685 people have been infected and 16 have died from the virus, the Web Site hoax forced authorities to deny it would isolate the entire territory. ...

<http://news.lycos.com/news/story.asp?section=Breaking&storyId=691262>

Ellison predicts major shakeout in Silicon Valley

"NewsScan" <newsscan@newsscan.com>

Wed, 02 Apr 2003 07:49:12 -0700

Oracle founder and CEO Larry Ellison says the high-tech industry is poised for another sweeping consolidation that will eliminate many of his rivals. "We think there's at least 1,000 Silicon Valley companies that need to go bankrupt," says Ellison, who predicted Oracle would be one of the survivors, along with Microsoft and IBM. He noted that nearly all software profits are generated by five companies (including Oracle), out of hundreds in the sector. Ellison says companies in Silicon Valley haven't come to grips with the realities of a maturing industry and have resisted the changes necessary to improve efficiency: "The whole model doesn't make sense. There's a bizarre belief that we'll be young forever." [*Wall Street Journal*, 1 Apr 2003; NewsScan Daily, 2 April 2003]
<http://online.wsj.com/article/0,,SB104923666370767900.djm,00.html>

(subscription required)

✦ Music piracy violations: \$150K a song

"NewsScan" <newsscan@newsscan.com>

Fri, 04 Apr 2003 09:07:26 -0700

The Recording Industry Association of America (RIAA) has filed lawsuits against four students it says it misappropriated academic computing resources to "illegally distribute millions of copyrighted works over the

Internet." Two of the accused students are enrolled at Rensselaer Polytechnic Institute, one student is enrolled at Princeton, and the fourth is at Michigan Technological University. If they are convicted, they could be fined as much as \$150,000 for each song they illegally traded. Digital media analyst Phil Leigh says of the RIAA's action: "This is just another step in the direction of demonstrating to the public that there will be penalties for what they consider to be copyright violations. I think they're attempting to take a carrot-and-stick approach here. They're whacking a few people with a stick now. And the carrot is the more liberal rules relating to label-backed subscription online services." [*San Jose Mercury News*, 4 Apr 2003; NewsScan Daily, 4 Apr 2003]
<http://www.siliconvalley.com/mld/siliconvalley/5558442.htm>

Streaming video: a patent on porn

Monty Solomon <monty@roscom.com>
Wed, 2 Apr 2003 10:07:00 -0500

Acacia Research says it owns five U.S. and 17 international patents covering the transmission and receipt of digital audio and digital video content, otherwise known as streaming media. But before attempting to enforce its patents with big outfits such as Yahoo! and The Walt Disney Co., Acacia instead chose to go after the smallish adult Internet sites that peddle videos of women (and men) doffing their clothes--and much more.

They sent letters to 700 racy Web sites with offers to arrange royalty deals, typically consisting of 1% to 2% of gross revenue. Do the deal or we'll see you in court, warned Acacia. Eight firms agreed to Acacia's terms. But 40 didn't, and Acacia promptly slapped them with lawsuits. Rather than buckling, though, several of the porno sites joined together and stood their ground. Now Acacia is in the fight of its life and may even face a shareholder revolt as a result. ... [Source: Seth Lubove, Forbes.com, 2 Apr 2003; PGN-ed]
http://www.forbes.com/2003/04/02/cz_sl_0402porn.html

⚡ Laws make crypto and untraceable E-mail illegal? (Re: [RISKS-22.66](#))

"Douglas W. Jones" <jones@cs.uiowa.edu>
Mon, 31 Mar 2003 13:45:24 -0600

[See items by Ed Felten (USE a Firewall, Go to Jail), Steve Bellovin and William Allen Simpson in [RISKS-22.66](#)). PGN]

[Some of this legislation] could have bizarre consequences for E-voting advocates, as well as for the entire Internet community.

I quote from Section 750.540c of the Michigan Penal Code, Full text online at:

<http://www.michiganlegislature.org/mileg.asp?page=getObject&objName=mcl-750-540c-amended>

This goes into effect today (March 31, 2003):

(1) A person shall not assemble, develop, manufacture, possess, deliver, offer to deliver, or advertise an unlawful telecommunications access device or assemble, develop, manufacture, possess, deliver, offer to deliver, or advertise a telecommunications device intending to use those devices or to allow the devices to be used to do any of the following or knowing or having reason to know that the devices are intended to be used to do any of the following:

(b) Conceal the existence or place of origin or destination of any telecommunications service.

(c) To receive, disrupt, decrypt, transmit, retransmit, acquire, intercept, or facilitate the receipt, disruption, decryption, transmission, retransmission, acquisition, or interception of any telecommunications service without the express authority or actual consent of the telecommunications service provider.

In effect, item 1b makes it illegal to create any anonymous communication service, and all of the interesting protocols for ballot deposit appear to rely on anonymization schemes of one kind or another.

Item 1c is really hard to make out. It appears to be intended as an anti-wiretapping rule, but the plain wording appears to require the express authority or actual consent of every ISP for any use of that ISP's facilities; does this mean that if I was in Michigan, I'd have to ask

permission before I hit the send key to E-mail this message? I checked their definition of telecommunications service provider and it is broad. The owner of the wire, the owner of the switching systems, they're all involved and each must give permission.

According to slashdot, a goodly number of states are now considering this kind of law. See:

<http://yro.slashdot.org/article.pl?sid=03/03/28/1541230&tid=103>

It's pretty obvious that they haven't thought these bills through.

✶ The reality behind these laws (Re: Firewall, Jail, [RISKS-22.66](#))

Fred Cohen <fc@all.net>

Tue, 1 Apr 2003 05:29:07 -0800 (PST)

As I read the Texas bill, it starts out by saying:

<http://www.capitol.state.tx.us/data/docmodel/78r/billtext/pdf/HB02121I.PDF>

"A person commits an offense if, with the intent to defraud a communications service..."

The Michigan bill starts out saying:

<http://www.michiganlegislature.org/printDocument.asp?objName=mcl-750-219a-amended&version=txt>

<http://www.michiganlegislature.org/printDocument.asp?objName=mcl-750-540c-amended&version=txt>

"(1) A person shall not knowingly obtain or attempt to obtain telecommunications service with intent to avoid, attempt to avoid, or cause another person to avoid or attempt to avoid any

lawful charge

for that telecommunications service by using any of the following:"

> The Bill analysis basically quotes the MPAA website!

> <http://michiganlegislature.org/documents/2001-2002/>

> billanalysis/house/htm/2001-HLA-6079-b.htm

This analysis agrees with mine. That these bills increase penalties only for already illegal actions and possibly criminalize what would currently be some civil matters. If you are paying for one class of service (e.g., home use of the Internet for one computer) and using it for another class of services (e.g., selling access to your neighborhood by putting up a NAT firewall), you are already violating the law and you will also be violating these laws.

I know that this was the April 1 issue, but the rumors on these bills are spreading faster than most computer viruses, and they have been spreading for several days with increasing intensity and are being taken seriously. Nothing in these bills in any way prevents firewalling, encryption, etc. UNLESS it is being used to defraud.

Fred Cohen - <http://all.net/> - fc@all.net - fc@unhca.com - tel/fax 925-454-0171

Fred Cohen & Associates - University of New Haven - Security Posture

[defraud ... in the eyes of the accuser! PGN]

✶ State Super-DCMAs will be suicidal (Re: [RISKS-22.66](#))

David Harmon <dmh@tiac.net>

Tue, 01 Apr 2003 11:23:41 -0500

I suspect at least the Michigan state legislature may reconsider -- after their tech industries pick up and *leave*. The first to go will be the ones actually working on the criminalized tools etc. These will be followed by those whose lawyers were paying attention. The third wave will be triggered as both government and private actors start (ab)using the new laws for arbitrary "takedowns" of their enemies. Of course, quickly repealing or nullifying the laws *may* stop the exodus, but I expect the state will still be regretting this bonehead move for some time, as will any other states who follow suit.

I do, however, doubt Massachusetts will actually *pass* any such law, given the assured and powerful opposition of MIT and their *many* friends. I would hope that whoever introduced it gets stomped at their next election, but that may be too much to ask. On the other hand, some of the other states in question may not have techies with enough pull to make their voice heard.

Of course, a fair number of the companies and persons involved will decide to leave the country altogether, leaving us with fewer national resources for defense *or* productivity. Steve Kirsch was right:

> The terrorists have won. They have successfully convinced America to

> attack itself.

(from: <http://www.skirsch.com/politics/iraq/Lessons911.htm>)

Dave H.

PS: The basic pattern I'm seeing here is that private self-defense "in cyberspace" is being methodically outlawed. Has anyone *else* noticed that "we" are slowly dismantling the various obstacles to a Handmaid's Tale style techno-coup?

⚡ Draft legislation on using crypto

"Peter G. Neumann" <neumann@csl.sri.com>

Mon, 31 Mar 2003 16:11:25 -0500

Cheating on income taxes or neglecting to pay sales taxes on online purchases could get you five extra years in prison if the government succeeds in restricting data-scrambling technology, and discourage human rights workers to protect sensitive data. Draft legislation circulating in the Justice Department would extend prison sentences for using encryption in the commission of a crime, something encryption advocates fear would achieve little in catching terrorists and hurt only legitimate uses of cryptography. The new proposal is part of the proposed Patriot II legislation. [Source: Anick Jesdanun, **The Washington Post**, 31 Mar 2003; PGN-ed via Dave Farber]

[The full item is available on Dave's IP Archives:

<http://www.interesting-people.org/archives/interesting-people/>

PGN]

✦ **Re: Draft legislation on using crypto ([RISKS-22.67](#))**

"David P. Reed" <dpreed@reed.com>

Mon, 31 Mar 2003 21:21:10 -0500

If they declare that encryptions are arms, perhaps we should point out the Second Amendment (favorite of the National Rifle Association) guarantees the right to keep and bear arms. [via Dave Farber's IP]

✦ **Patriot software again a concern?**

"Robert I. Eachus" <rieachus@attbi.com>

Mon, 31 Mar 2003 19:53:22 -0500

The two Patriot "failures" in have different -- and understandable -- modalities. Whether these incidents were indicative of a problem with the system has to be determined. The first thing you have to understand is that once a missile has been fired, if an aircraft flies between the target and the Patriot radar on the ground, the missile can acquire the closer aircraft. The Patriot operator can tell the radar not to track the closer aircraft when that plane is showing friendly IFF. If this happens, the

missile

should reacquire the original target. Off course, if the missile is close to the aircraft, the wrong target may be attacked anyway.

This seems to be what happened in the incident where the British aircraft was shot down. It is not clear whether there really was an enemy missile -- or if the incoming was really a mortar shell.

The decision to put IFF recognition in the Patriot ground systems but not in the missiles is both a practical design decision and a military one. If the enemy starts broadcasting "your" IFF code do you want the Patriot system to be able to override IFF recognition?

In the second incident, the operators were again under attack and apparently "unassed" the control trailer. My guess is that the radar was in TWS (track while scan) mode, and the F-15 countermeasures read it as a lock-on -- which of course it was. If the Patriot battery had been manned they could have either told the radar not to lock on to the F-15, or turned off the radar so that the HARM would have lost lock.

In both cases, note that the situation was a typical one for "friendly fire" incidents -- multi-mode attacks that haven't been considered by the rules of engagement.

⚡ Friendly Fire and the Perils of Statistical Reasoning

Thomas A. Russ <tar@ISI.EDU>
31 Mar 2003 15:02:39 -0800

Actually, having it be higher in the first Gulf War is not really that astounding, given the general circumstances. In that war, the overwhelming majority of all casualties were inflicted by the Coalition Forces. Given that tremendous disparity, even a very small error rate applied to the casualty causation numbers would end up being a very large part of the overall casualties.

While good figures for the Iraqis are hard to come by, CNN's web site lists the following. Coalition 213 combat fatalities (plus another 145 nonbattle deaths). Iraqi military fatalities estimated at 100,000. If the latter is true, then having just a 0.1% error rate would explain about 100 friendly casualties or about half of all of them...

(CNN did not break down US casualties by cause, although British losses were listed as 24, 9 by U.S. fire).

Thomas A. Russ, USC/Information Sciences Institute
tar@isi.edu

✶ Re: Friendly fire ([RISKS-22.65](#))

Anthony Youngman <Anthony.Youngman@ECA-International.com>
Mon, 31 Mar 2003 10:27:41 +0100

In the first Gulf War, our (the British) "friendly fire" casualties were

about FIFTY percent of total casualties. Nearly all of them were caused by a single American "hunter air patrol" which, while OUT of its patrol area, and OUT of radio touch (accidental or deliberate?) with its controllers, mis-identified two Warrior APCs as Iraqi and destroyed them.

It caused considerable bad press over here, and the impression left was that the pilots were fed up with not finding targets, wanted to attack something/anything, and had pretty much disobeyed orders in order to find something to shoot at. Shame it was a bunch of soldiers on the same side ...

✶ NCIC: "Death by Oops?"

Lauren Weinstein <lauren@vortex.com>
Wed, 02 Apr 2003 20:34:30 -0800 (PST)

The latest "Fact Squad Radio" short audio segment may be of interest. It concerns the issue of data accuracy in the FBI's NCIC system. It's called:

"The FBI NCIC: Death by Oops?"
and is available via:

<http://www.factsquad.org/radio>

+1 (818) 225-2800 lauren@pfir.org
PFIR: People For Internet Responsibility - <http://www.pfir.org>

✶ POW Social Security numbers revealed

Paul Hirose <x3xpp-c52ye-0401@earthlink.net>

Thu, 03 Apr 2003 00:02:47 GMT

The current war in Iraq has highlighted a risky practice the Pentagon has been following for many years: using the Social Security number as a military member's "service number". Americans taken POW have been seen and heard on television identifying themselves as required by the Geneva Convention. Naturally this included reciting their SSNs.

In every case I've seen (all on American TV), the interview was edited so only the first few digits were revealed. I'm not sure who did this; I hope it occurred at the source (presumably Iraqi state television).

The use of SSNs as service numbers was an issue even before the war. In one incident, some senior officers suffered identity theft when their SSNs were published in the Congressional Record:

<http://www.washingtonpost.com/ac2/wp-dyn/A35194-2000Apr7?language=printer>

Foreign readers should understand the SSN is practically an American's national identity number, heavily used by the government, employers, banks, even schools. Broadcasting a POW's name and SSN worldwide creates a severe risk of identity theft and invasion of privacy.

Perhaps when the change to SSNs occurred (in the Vietnam era, according to the newspaper article) the danger seemed minimal. But times have changed. The Pentagon should revert to service numbers which have no meaning or usefulness outside the military.

Paul Hirose <x3xpp-c52ye-0401@earthlink.net>

✶ Cell phones & 911 service

Jeremy Epstein <jeremy.epstein@webmethods.com>

Wed, 2 Apr 2003 10:54:10 -0500

The Washington Post reports on a number of cases where calling 911 from a cell phone was routed to the wrong jurisdiction, so "response to a life-threatening -- and ultimately fatal -- emergency was delayed because a cell phone call to 911 didn't work the way it was supposed to".

The examples given were a caller in Chillum MD routed to 911 in Washington

DC (an immediately adjacent jurisdiction) and the recent case [[RISKS-22.58](#)]

where teenagers in Long Island Sound drown because 911 wasn't able to

determine where the call was coming from. They note that in the Chillum

case, the problem occurred because "a wireless signal can get picked up by

the wrong cell phone tower".

In this case, though, the technology isn't at fault, despite what *The Post*

says. Radio waves don't respect human boundaries; the cell phone goes to

the nearest/strongest signal (not sure exactly how this works).

If I stand

on one side of a street, I can be in a different jurisdiction from the other

side of the street. There's no way for the cell tower to know which side of

the street I'm on, and route the call to the correct 911 location. The RISK is that 911 dispatchers aren't trained to recognize calls from adjacent jurisdictions and route them appropriately.

<http://www.washingtonpost.com/wp-dyn/articles/A54802-2003Mar30.html>

✶ Possibly-wrong expectations about bouncing e-mail

"Mark T.B. Carroll" <Mark.Carroll@Aetion.com>
Fri, 4 Apr 2003 07:50:16 -0500 (EST)

I have domain names with short names where all e-mail to anyone at that domain comes past me. One thing I find is that people from organisations that have a similar domain name to one of mine send their inter-office stuff to me as they mistype their own organisation's domain name in the intended recipients' addresses. I wonder if they would be more careful with internal documents if they realised it is actually not all that improbable that e-mail to Some.Odd.Name@wrong-short.domain that doesn't look like spam will be read by at least somebody instead of being bounced automatically.



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 68

Saturday 12 April 2003

Contents

- [IBM's DB2 blamed for Danish banking crisis](#)
[Fuzzy Gorilla](#)
- [Man Gets \\$12,000 Electric Bill](#)
[Fuzzy Gorilla](#)
- [Missile-defense test failure linked to a single chip](#)
[Fuzzy Gorilla](#)
- [Millennium trains taken off the tracks](#)
[John Colville](#)
- [Stupid Security Awards for 2003](#)
[Simon Davies](#)
- [Radio stations unable to play copy protected CDs](#)
[Jeffrey Sunseri](#)
- [Net fraud complaints triple in 2002](#)
[Keith Rhodes](#)
- [Credit-card theft](#)
[sergioch](#)
- [Re: Friendly Fire](#)
[Peter B. Ladkin](#)
[Rod Van Meter](#)
[David Guaspari](#)

- [Re: The reality behind these laws](#)
[Stanislav Shalunov](#)
 - [Re: POW Social Security numbers revealed](#)
[Jaanus Kase](#)
[Crispin Cowan](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ IBM's DB2 blamed for Danish banking crisis

"Fuzzy Gorilla" <fuzzygorilla@euroseek.com>
Sun, 06 Apr 2003 11:54:03 -0400

Danske Bank is pointing fingers at IBM's DB2 database as the culprit for a massive outage that caused the Danish bank's trading desks, currency exchange and communications with other banks to shut down. The problems began on 10 Mar 2003, when a defective power unit was replaced in an IBM Ramac Virtual Array (RVA) storage system. An electrical outage occurred during the repairs, which caused operations at one of the bank's two operating centers to come to a halt. When operations were finally resumed, extensive data inconsistencies were discovered throughout a week-long process of trying to recover data. Apparently, a flaw had existed in DB2 in comparable installations since 1997, although it had not been detected prior to this event. IBM has issued a fix. [Source: Ashlee Vance, The Register, 4 Apr 2003; PGN-ed]
<http://www.theregister.co.uk/content/53/30095.html>

⚡ Man Gets \$12,000 Electric Bill

"Fuzzy Gorilla" <fuzzygorilla@euroseek.com>

Fri, 04 Apr 2003 16:31:11 -0500

On April Fools' Day, Randy Carrol in North Platte, Nebraska, received an electric bill of \$12,344.16 for 33 days' service. But it was not a joke -- except that the amount was generated by new billing software, showing use of 310,421 kilowatts (instead of the usual 300). The correct amount due later turned out to be \$26.26. [Source: AP item, 4 Apr 2003; PGN-ed] http://story.news.yahoo.com/news?tmpl=story2&u=/ap/20030404/ap_on_fe_st/electric_bill

⚡ Missile-defense test failure linked to a single chip

"Fuzzy Gorilla" <fuzzygorilla@euroseek.com>

Fri, 11 Apr 2003 20:39:09 -0400

According to Jack Kelble, president of Raytheon Space and Airborne Systems, the failure of a U.S. missile-defense test on 11 Dec 2002 was caused by the malfunction of a single chip that failed to signal an exo-atmospheric kill vehicle to separate from its booster rocket. Coming just five days before Presidential directive on speeding deployment of missile defenses, the test included the use of Navy Aegis cruisers and a Boeing 747 modified as the Airborne Laser Lab. Both were used as trackers for the

Minuteman II ICBM

launched from Vandenberg Air Force Base, California, as a target missile.

Each flight test costs an average of \$100 million. [Source: Loring Wirbel, EE Times, 11 Apr 2003; PGN-ed]

<http://www.eetimes.com/sys/news/OEG20030410S0066>

✶ Millennium trains taken off the tracks

John Colville <colville@it.uts.edu.au>

Fri, 11 Apr 2003 13:47:26 +1000

The Millennium trains (so-called because of when they were supposed to start running, although that was delayed until ten months ago in mid-2002) have been taken out of service indefinitely, due to electrical problems that were having a "flow-on effect across the Sydney network." Train signals were interfering with the frequency of the underground signalling system resulted in turning lights red for following trains. Only four 8-car trains have been delivered thus far (out of the contracted 81, with a total cost of 232 million Australian dollars). Transport Services Minister Michael Costa said, "This is the most complex train that's ever run on a rail system. It is a piece of equipment that would, in the normal course of events, have some teething problems." Other problems were also cited: passenger doors occasionally refusing to close; loss of the public address system; and loss of air-conditioning in some units. [Source: Joseph Kerr and

Darren Goodsir,

Sydney Morning Herald, 10 Apr 2003; PGN-ed from JC's
excerpting]

<http://www.smh.com.au/articles/2003/04/10/1049567807326.html>

John Colville, Dept of Computer Systems, University of
Technology, Sydney
Broadway NSW Australia 2007 colville@it.uts.edu.au +61-2-9514-
1854

✶ Stupid Security Awards for 2003

Simon Davies <s.g.davies@lse.ac.uk>

Tue, 8 Apr 2003 20:20:30 +0100

Privacy Watchdog announces winners of competition to find the
world's most
stupid security measures; Global quest has identified absurd and
pointless
security requirements

Privacy International today announced the results of its
competition to find
the worlds most pointless, intrusive and egregious security
measures. The
competition, launched in February, attracted almost 5,000
nominations from
35 countries. While the air security sector dominated the
competition,
nominations arose from almost all areas of private and public
sector
activity. The winners include JFK Airport, T-Mobile (UK),
Michigan
Correctional facilities and the Australian Government.

The "Stupid Security" award was judged by a distinguished
international
panel of security and privacy experts and is intended to

highlight the absurdities of the security industry. Privacy International's director, Simon Davies, said his group took the initiative because of "innumerable" security initiatives around the world that had absolutely no genuine security benefit.

"The extraordinary number of nominations indicates that the situation has become ridiculous" said Mr Davies. "Security has become the smokescreen for incompetent and robotic managers the world over. The situation has become more than an irritation to the public. It has become an outright danger".

The winners are:

Most Egregiously Stupid Award

* Winner: The Australian Government for a litany of pointless, irritating and self-serving security measures

* Runner-Up: Moscow Mayor Yury Luzhkov for the 'Propiska' Identity Papers

Most Inexplicably Stupid Award

* Winner: Philadelphia International Airport for over-reaction to a bottle of cologne

* Runner-Up: Heathrow Airport for quarantining a quantity of green tea

Most Annoyingly Stupid Award

* Winner: T-Mobile (UK) for pointless and idiotic financial security measures

* Runner-Up: Bay Area Rapid Transport (Bart) for closing its

restrooms.

Most Flagrantly Intrusive Award

* Winner: Delta Terminal at JFK Airport for forcing a nursing mother to drink still-warm bottles of her own breast milk

* Runner-Up: Carson City Correctional Facility, Michigan for forcing women visitors to wear bras.

Most Stupidly Counter Productive Award

* Winner: San Francisco General Hospital for blind idiocy in its identity checking procedures

* Runner-Up: San Francisco International Airport for endangering the public

* Dishonourable Mention: The New Yorker Hotel, New York for aggressive, unnecessary and meaningless security measures.

Full details at <http://www.privacyinternational.org/activities/stupidsecurity/>

Simon Davies can be reached at simon@privacy.org Phone (+44) 7958 466 552

[Note 1: Privacy International (PI) <http://www.privacyinternational.org> is a human rights group formed in 1990 as a watchdog on surveillance by governments and corporations, including wiretapping and national security activities, ID cards, video surveillance, data matching, police information systems, and medical privacy.]

[Note 2: (Disclaimer) PGN was one of the judges.]

✶ Radio stations unable to play copy protected CDs

"Jeffrey Sunseri" <JSunseri@mtaloy.edu>

Mon, 07 Apr 2003 15:09:20 -0400

Music companies which use copy protection may be denying the artists under contract to them legitimate play time on radio stations, if the happenings at one outfit are any indication. [First sentence on Declan's Politech]

[Some radio stations with desktop PCs rather than standalone CD players are unable to play the free CDs they get from EMI because of disc copy protection. PGN-ed of the article]

<http://www.theage.com.au/articles/2003/04/03/1048962867084.html>

✶ Net fraud complaints triple in 2002

Keith Rhodes <rhodesk@gao.gov>

Fri, 11 Apr 2003 04:59:58 -0700 (PDT)

The FBI's Net fraud unit says it referred 48,000 complaints to law enforcement last year, with both the number of fraud cases and the dollar loss associated with them more than tripling. [Source: Paul Festa, CNET News.com, 10 Apr 2003]

http://zdnet.com.com/2100-1105-996270.html?tag=sas_email

Credit-card theft

<sergioch@ciaoweb.it>

Sat, 12 Apr 2003 11:42:37 +0200

A mailman in Settimo Torinese (a small town in northwestern Italy) has robbed several credit cards and the relative letters with the PIN. His theft was found after one of the owners of the cards discovered that 3000 euros were missing from her account due to shopping made with her card, which she had never received. The police searched the home of the thief. It found more than 100 (a hundred) letters communicating the PIN code to the owners of the cards, plus for an amount of about 5000 euros in bought articles (mainly in sportswear, we are told).

"The "Servizi Interbancari" (interbanking services), Italian leader in credit card management, told that it is the first time that such event occurs in Italy and that <<highest security guidelines>> are followed in the dispatch of cards and PINs."

Sarcasm is left to the reader as an exercise.

Sources (in Italian):

La Stampa, 11/04/2003, cronaca di Torino (page 41).

http://www.lastampa.it/search/albicerca/ng_articolo.asp?IDarticolo=782728

Google Translation (not great):

http://translate.google.com/translate?u=http%3A%2F%2Fwww.lastampa.it%2Fsearch%2Falbicerca%2Fng_articolo.asp%3FIDarticolo%3D782728&langpair=it%7Cen&hl=it&ie=ISO-8859-1&prev=%2Flanguage_tools

Re: Friendly Fire ([RISKS-22.65](#) to [22.67](#))

"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>

Mon, 07 Apr 2003 11:22:55 +0200

Recent "friendly fire" incidents (known in the military as fratricide) were introduced in [RISKS-22.65](#) by Paul, and discussed in [RISKS-22.66](#) by Tyson and [RISKS-22.67](#) by Eachus, Russ, and Youngman.

Chris Johnson of the Accident Analysis Group at the University of Glasgow has an review article on the subject [1]. He recently quoted the following percentages of all reported casualties sustained, from FM100-14, US Army, 1998:

	World War II	Korea	Vietnam	Desert
Storm/Shield	(1942-45)	(1950-53)	(1965-72)	(1990-
1991)				
Accidents	56%	44%	54%	75%
Friendly Fire	1%	1%	1%	1%
Enemy Actions	43%	55%	45%	20%

As Russ pointed out, it is important not just to view percentages but also to know the absolute numbers, as asserted by 100% of the people typing this note, who doesn't have those numbers available.

A particularly noteworthy fratricide incident occurred in 1994 during Operation Provide Comfort, which intended to protect certain Kurdish areas in Northern Iraq. Two F-15s patrolling the no-fly zone shot down

two Black

Hawk helicopters ferrying officials and locals within the no-fly zone. This

incident has been analysed by (in temporal order) a USAF Aircraft Accident

Investigation Board, by a US General Accounting Office review of that report

[2], by U.S. military academician Scott Snook [3], by Joan Piper, the mother

of one of the officers killed [4], and by Nancy Leveson, Polly Allen and

Margaret-Anne Storey [5].

During the incident, the major technologies involved were a controlling

AWACS aircraft, and the Air-to-Air Interrogation/Identification Friend or

Foe (AAI/IFF) systems on board the F-15s and the Black Hawks, systems which

send radio interrogation signals (AAI) and elicit responses (IFF) from

friendly aircraft. These systems are similar in function to that of the

combination of Primary Air Traffic Control Radar and on-board transponders

in civil aviation, although I expect the military security design is far

more sophisticated.

During this incident, the technology apparently functioned more or less as

intended, although there was some question as to why certain AAI/IFF

transactions did not occur, which has not been answered.

(Although the

F-15s were interrogating on a different band from that on which the Black

Hawks were responding, at least one performed interrogation should have

elicited a response. No reason for this was identified.)

When the F15 pilots failed to get suitable responses from AAI/IFF transactions, they performed a visual intercept, mistakenly

identified the Black Hawks as Iraqi Hind helicopters, and shot them down. The reports focused on procedural irregularities (problems in the chain of command during the intercept), on coordination on board the AWACS, and the apparent haste, inaccuracy, and lack of procedural care with which the F15s performed the visual identification and shootdown. The GAO also investigated mission discipline issues with the squadron to which the interceptors belonged.

According to the GAO, the USAF report "focused on, among other things, command and control problems, including individuals' lack of knowledge of specific procedures." The GAO report pointed out that the USAF report did not discuss the F-15 pilots' responsibility to report to the Airborne Command Element (ACE, the chief of the AWACS operation staff) when they encountered unknown aircraft in the no-fly zone; that it failed to note that the ACE had authority to stop the intercept (especially significant given that his staff had been dealing with those same helicopters a short while before); and that it erroneously concluded that use of an incorrect "squawk" code by the Black Hawks resulted in the F15s not receiving an IFF response (the F15s should have seen a response in any case on at least one of their required interrogation modes).

These seem to me to be problems largely concerning organisational behavior rather than the technology itself, although this behavior is of course conditioned by that technology. One could expect this to be so

in general
for fratricide incidents, since, except for intentional incidents such as "fragging", they are cases of mistaken identity and are thus likely to contravene the rather elaborate procedures that have evolved for avoiding it.

Another case, investigated by the organisational behavior researcher Gene Rochlin [6], was the shootdown of a commercial aircraft, an Iran Air Airbus Flight 655, over the Persian Gulf by an Aegis cruiser, the USS Vincennes, who was engaged in a firefight at the time with small Iranian patrol boats. The aircraft was initially misidentified as an F14, and its subsequent behavior was misinterpreted as threatening, despite the wealth of electronic information available to the Aegis crew which showed otherwise - a case of seeing what one expects (or fears) to see, it seems. Again, organisational behavior, conditioned by the available technology.

The recent Patriot shootdown of a RAF Tornado may be different, in that it may have been initiated by technological malfunction. According to Flight International [7], "the aircraft was approaching the Kuwaiti border as number two in a two-ship formation when it was identified by the Patriot as an anti-radiation missile. An operator then initiated the engagement, before realising that other sensor data did not corroborate the target classification. Initial indications are that the Tornado was in the "safe-lane" at the right speed and height when it was hit. If it had an IFF problem, even not functioning or broadcasting the wrong

identification tag,
it would probably still have been spotted by the airborne
control post."

The report continues: "Further doubts were raised about
Patriot's IFF system
when a day later a second SAM battery, 55km (35 miles) south of
An Najaf,
locked on to a US Air Force F-16. The fighter fired a [anti-
radiation
missile], destroying the battery's radar without killing anyone.

References

[1] Chris Johnson, Risk and Decision-Making in Military Accident
and

Incident Reporting Systems, available at

<http://www.dcs.gla.ac.uk/~johnson/papers/Military.pdf>

[2] General Accounting Office, USG, Operation Provide Comfort:
Review of
U.S. Air Force Investigation of Black Hawk Fratricide Incident,
Report to
Congressional Requestors, Report GAO/OSI-98-4, November 1997,
available
through search from <http://www.gao.gov>

[3] Scott A. Snook, Friendly Fire: The Accidental Shootdown of U.
S. Black

Hawks over Northern Iraq, Princeton University Press, 2000.

Details at

<http://pup.princeton.edu/titles/6847.html>

[4] Joan L. Piper, A Chain of Events: The Government Cover-Up of
the Black

Hawk Incident and the Friendly-Fire Death of Lt. Laura Piper,
Brassey's Inc,
2001.

[5] Nancy G. Leveson, Polly Allen, Margaret-Annd Storey, The
Analysis of a

Friendly Fire Accident using a Systems Model of Accidents,
available from

<http://sunnyday.mit.edu/accidents/>

[6] Gene I. Rochlin, Iran Air Flight 655: Complex, Large-Scale Military

Systems and the Failure of Control. In Responding to Large Technical

Systems: Control or Anticipation, Renate Mayntz and Todd R. La Porte, eds.,

Kluwer, 1991. A version is also to be found as Chapter 9 of Rochlin, Trapped

in the Net, Princeton University Press, 1997, which chapter is available at

http://pup.princeton.edu/books/rochlin/chapter_09.html

[7] Accidents Take Their Toll, Flight International, 1-7 April 2003, p6.

Peter B. Ladkin, Faculty of Technology, University of Bielefeld, 33594 Bielefeld, Germany +49 (0)521 880 7319 <http://www.rvs.uni-bielefeld.de>

✦ Re: Friendly Fire ... (Russ, [RISKS-22.67](#))

Rod Van Meter <Rod.VanMeter@nokia.com>

04 Apr 2003 14:55:01 -0800

I'm not certain where Mr. Russ got his data, but as of 14:30 PST on 4 Apr,

<http://www.cnn.com/SPECIALS/2003/iraq/forces/casualties/index.html> lists 84

coalition deaths and another couple of dozen POW/MIAs. It also seems

unlikely that we have already killed a full four tenths of a percent of the

population of Iraq. I don't see numbers for injured at a glance.

The problem likely stems from confusion over the term "casualty". It

actually refers to persons killed OR INJURED, although many people seem to believe it refers to deaths.

The same issue has caused over fifty years of misinformation about the atomic bombing of Japan and the planned Operation Olympic invasion of Japan's home islands, due to confusion over casualties on Okinawa and Iwo Jima.

⚡ Re: Friendly fire ... (PGN, [RISKS-22.65](#))

David Guaspari <davidg@atc-nycorp.com>

Mon, 7 Apr 2003 16:21:48 -0400

It would take some hard work to decide whether [a high friendly fire rate] is astounding or is a simple statistical necessity. If side A so overmatches side B that B can do A no damage at all, then 100% of A's casualties will be the result of friendly fire (or self-inflicted by other kinds of accident).

David Guaspari, ATC-NY, 33 Thornwood Drive, Suite 500, Ithaca NY 14850-1250

voice: (607) 266-7114 davidg@atc-nycorp.com

⚡ Re: The reality behind these laws (Re: Cohen, [RISKS-22.67](#))

stanislav shalunov <shalunov@internet2.edu>

04 Apr 2003 15:30:20 -0500

> Nothing in these bills in any way prevents firewalling,
encryption,
> etc. UNLESS it is being used to defraud.

I certainly hope that this was the intent. However, the law says:

> Sec. 540c (1) A person shall not [...] assemble,
> develop, manufacture, possess, deliver, offer to
> deliver, or advertise a telecommunications device
> intending to use those devices or to allow the
devices
> to be used to do any of the following or knowing
or
> having reason to know that the devices are
intended to
> be used to do any of the following: [...]

> (b) Conceal the existence or place of origin or
> destination of any telecommunications
service.

A NAT box is a telecommunications device. Some common home WiFi access points can *only* be used in NAT mode, such as a few Linksys boxes. A NAT box is intended to conceal the actual origin of IP traffic. IP traffic seems to fit their definition of a telecommunications service. It would seem that the possession of a NAT box is made a felony in Michigan, punishable by up to four years in prison and/or up to \$2000 fine per device. Please explain where you are reading this ``intent to defraud'' stuff? (Sec 219a does use ``with the intent to defraud'' language carefully, but we're talking about a different section here. Are we reading different texts? I'm talking about
<URL:<http://www.michiganlegislature.org/printDocument.asp?>

[objName=mcl-750-540c-amended&version=txt>.](#))

My reading of this is that it outlaws (both sale and possession) of NAT and VPN boxes and perhaps more (steganography?). Note that there does not need to be any malicious intent in order for the possession to be illegal.

In addition, the item (c) that immediately follows is written quite vaguely (it was probably meant to outlaw cable descramblers), but it written -- probably unintentionally -- so that it might be interpreted as outlawing (the decryption side of) any use of encryption without prior permission from the service provider (all of them on the path, I guess?).

Stanislav Shalunov <http://www.internet2.edu/~shalunov/>

✦ Re: POW Social Security numbers revealed (Hirose, [RISKS-22.67](#))

"Jaanus Kase" <terminus@local.ee>
Sat, 5 Apr 2003 01:45:07 +0300

Foreign readers, like myself, are well aware of America's problems with SSN. To my view, the problem is very simple: identification and authentication are two very different issues, but SSN is used for both.

Let's face it: to have efficient public services and efficient means of communications in current Internet age and information society, it is vital

to have a sort of universal "national identity number", whatever it is called - ID code, SSN, "medical insurance code" or whatever. They are often used in medical or social insurance, but not necessarily always - it can be used when providing any service or just wanting to talk to someone to be sure of his identity.

I myself live in Estonia and I think we have a good national ID code system in place. Every person has a unique code - for example, mine is 38006270262. I can tell it to you freely, because it is available online anyway in a lot of places. It is widely accepted here that the ID code is public data. Think of it as your middle name. It is even helpful in daily electronic communications - if you have two persons with the same name, you can distinguish them by the code. It is also obvious that all sorts of electronic registers are easy to construct using the code. In itself, the ID code also encodes some key personal data, like your birth date and sex, but nothing else.

A direct result of the above is that the code must NOT be used for authentication purposes. If I know someone's name and ID code, I should NOT be able to impersonate as that person. Indeed, all services in Estonia, public or private, consider this and knowing only someone else's name and/or ID code gets you nowhere - additional authentication is always used.

As I view it, the core of US problems with SSN is very simple - it is used widely as a unique identifier as it is very easy to do so (as, I

understand,
it is the only numeric identifier that all US residents can be
assumed to
have). And then, you play hide-and-seek and say, "okay, the
number is
everywhere all over the place anyway, but now let's play it's
secret and
start authenticating people using it."

I of course understand that the US system is in its current
state due to its
historic legacy, but in the long run, some changes will probably
need to be
made, although I wouldn't want to imagine the costs. You may say
that there
are valid arguments against having a universal public national
ID code, but
so far, I have not seen any, either in talk or in practice, that
I would
take seriously.

✉ Re: POW Social Security numbers revealed (Hirose, [RISKS-22.67](#))

<crispin@wirex.com>

Fri, 04 Apr 2003 19:32:26 -0800

It is often suggested that disclosure of SSN's is a great risk.
In the
current climate, where SSN's are used to *authenticate* an
individual ("tell
us your SSN so we know it is you") that certainly is true.

However, I suggest an alternate approach to solving the problem
of identity
theft. SSN's are hopelessly easy to obtain; attempting to
curtail the
broadcast of these numbers (e.g. hoping the Iraqi state

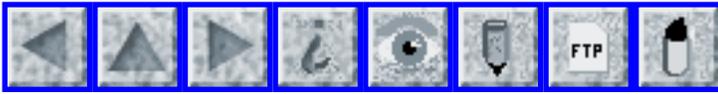
television will
control the release) is futile. Instead, I suggest that the US
Government
prohibit the use of SSN's as authenticators. If all of the US
organizations that currently authenticate with SSN's were forced
to use
something else (anything else) the state of the identity theft
crisis would
improve drastically.

The "*anything* else" part is important to this proposal. It is
tempting to
propose something prescriptive, specifying how organizations
should
authenticate people. However, I suspect that such prescriptions
would make
the law founder on impracticality, as organizations find high
quality
authentication difficult to implement for one reason or another.

In contrast, simply forcing organizations to choose something
else at least
has the scattershot effect that they are unlikely to choose all
the same
attributes, making wholesale identity theft much more difficult.

Just me proposing this idea here and getting a few folks to
agree that it
would be beneficial is fun & all :-) but won't actually change
anything. More constructive would be if those who do agree with
the idea,
and have more influence in the financial regulation space than I
do, would
take up the idea and start spreading it around.

Crispin Cowan, Chief Scientist, WireX <http://wirex.com/~crispin/>
<http://wirex.com> [http://h18000.www1.hp.com/products/servers/
solutions/iis/](http://h18000.www1.hp.com/products/servers/solutions/iis/)



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

[ACM](#) Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 69

Tuesday 15 April 2003

Contents

- [NSW forced to hand count poll result](#)
[Chris Maltby](#)
- [Web Site for posting local election results crashes after virus attack](#)
[Monty Solomon](#)
- [UK Demon ISP suffers three-fold power loss](#)
[Walter Roberson](#)
- [Nevada hospital system hack traced to Russia](#)
[Monty Solomon](#)
- [Automated denial-of-service attack using the U.S. Post Office](#)
[Bruce Schneier via Monty Solomon](#)
- [Risks posed by online systems for college and graduate admissions](#)
[Matt Hiller](#)
- [Paypal Meets the Patriot Act](#)
[Solveig Singleton via Hanah Metchis](#)
- [Risks of *not* being lost](#)
[David Lesher](#)
- [Nova Scotia police track suspect with GPS](#)
[M Taylor](#)
- ["Quick Deposit" systems](#)
[Gervase Markham](#)

- [Double-barrelled surname costs disabled mother](#)
[Nigel Metherringham](#)
 - [New, comprehensive Federal rules on privacy of medical information](#)
[Jack Goldberg](#)
 - [75+ organizations urge FBI NCIC database accuracy](#)
[Marc Rotenberg](#)
 - [Re: POW Social Security numbers revealed](#)
[Crispin Cowan](#)
 - [Re: The reality behind these laws](#)
[Bill Gunshannon](#)
 - [Re: Millennium trains taken off the tracks](#)
[Bob Frankston](#)
 - [Re: Friendly Fire](#)
[Peter B. Ladkin](#)
[Allan Goodall](#)
 - [Changing Domain Registration info without verification](#)
[risks@Orwellian.Org](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ NSW forced to hand count poll result

Chris Maltby <chris@sw.oz.au>
Mon, 14 Apr 2003 18:24:16 +1000

"Computer problems have forced the New South Wales electoral office to start manually counting nearly 4 million upper house ballot papers. NSW Electoral Commissioner John Wasson says it will be a mammoth task to have all the votes counted and preferences allocated before the declaration of the poll at the end of the month. It is hoped the computer glitches will be fixed later this week, but Mr Wasson says he can not afford to delay

the count any longer. [...]

<<http://www.abc.net.au/news/justin/nat/newsnat-14apr2003-43.htm>>

My (slightly informed) guess is that the NSW Electoral Office acquired and made changes to the Australian Electoral Commission's election management software. The changes are to allow for the new NSW Upper House voting system and they have not been a success. This is probably due to inadequate testing as the changes to the Electoral Act were made quite some time ago.

To give them some credit, it's quite a challenge to simulate an election with 4 million voters in a realistic way. My experience with testing the AEC software in the pre-outsourced mid-1990s was that the stresses imposed by a real election were always well in excess of anything that could be simulated -- and some elections were conducted with changes to the counting requirements made in the last few months before the election...

I'll bet he's hoping the software starts working though. Mind you, it's hard to be all that confident in the results -- even leaving aside that the requirement for random sampling of papers in NSW upper house elections (unlike the Senate) makes exact reproduction of results problematic.

The return of the writs is required by 29 Apr 2003 IIRC.

Web Site for posting local election results crashes after virus attack

Monty Solomon <monty@roscom.com>

Sun, 13 Apr 2003 01:30:50 -0400

A Web site designed to tally and publish the results of a local election in Will County, Illinois was unable to perform as expected because it was deluged with phony requests. The Will County Director of Information Systems has informed the FBI.

<http://www.theage.com.au/articles/2003/04/07/1049567599656.html>

[Excerpted from SANS NewsBites April 9, 2003 Vol. 5, Num. 14

http://www.sans.org/newsletters/newsbites/vol5_14.php

along with Eugene Schultz's Editor's Note:

Although this news item might superficially appear to not be all that

important, it is really quite significant. There is considerable

apprehension concerning computerized voting systems, and incidents such

as this one will only increase the level of concern. ES]

UK Demon ISP suffers three-fold power loss

Walter Roberson <roberson@ibd.nrc.ca>

Tue, 15 Apr 2003 00:24:30 -0500 (CDT)

The UK ISP Demon suffered a multiple-failure power loss that left them with a backlog to process afterwards. The public grid went down, the backup generator had a control problem, and the standby batteries ran out before replacement parts for the generator could be located.

<http://www.theregister.co.uk/content/6/30194.html>

✦ Nevada hospital system hack traced to Russia

Monty Solomon <monty@roscom.com>

Sun, 13 Apr 2003 01:30:52 -0400

The security of a small Nevada hospital's computer system was breached by a hacker who has been traced back to Russia. The hacker routed the attack through the al-Jazeera Web site to make it look as if the attack came from the Middle East. The hacker may have accessed employees' social security numbers and bank account information. A Trojan horse program embedded in a game some employees had downloaded allowed the attackers access. The hospital's payroll system has been removed from the network and employees have been instructed never to install software or sign on to streaming Internet services.

[Source: *USA Today*, 7 Apr 2003

http://www.usatoday.com/tech/webguide/internetlife/2003-04-07-hospital-hack_x.htm

excerpted from SANS NewsBites April 9, 2003 Vol. 5, Num. 14

http://www.sans.org/newsletters/newsbites/vol5_14.php

along with Eugene Schultz's Editor's Note:

Employees installing software or signing on to streaming Internet

services may have been a problem, but I wonder whether the hospital's

failing to set requirements for and failing to enforce a baseline level

of security may have had a lot to do with what happened here. ES]

⚡ Automated denial-of-service attack using the U.S. Post Office

Monty Solomon <monty@roscom.com>

Mon, 14 Apr 2003 03:33:40 -0400

In December 2002, the notorious "spam king" Alan Ralsky gave an interview.

Aside from his usual comments that antagonized spam-hating e-mail users, he

mentioned his new home in West Bloomfield, Michigan. The interview was

posted on Slashdot, and some enterprising reader found his address in some

database. Egging each other on, the Slashdot readership subscribed him to

thousands of catalogs, mailing lists, information requests, etc. The

results were devastating: within weeks he was getting hundreds of pounds of

junk mail per day and was unable to find his real mail amongst the deluge.

Ironic, definitely. But more interesting is the related paper by security

researchers Simon Byers, Avi Rubin and Dave Kormann, who have demonstrated

how to automate this attack.

[Source: Bruce Schneier's cryptogram]

<http://www.counterpane.com/crypto-gram-0304.html#1>

⚡ Risks posed by online systems for college and graduate admissions

Matt Hiller <hiller@panix.com>

Mon, 14 Apr 2003 11:28:52 -0700 (PDT)

Late last year, I sent out a number of applications to masters programs in computer science. Where possible, I submitted my applications by way of online application systems, and had my recommendation providers submit their recommendations online. (In fact, a number of programs charge an increased application fee to applicants who choose to submit their applications on paper rather than using the online system; paper seems to be deprecated.) I did not realize that in doing this I was exposing myself to a significant computer-related risk, as illustrated by my experience with the University of Virginia.

I applied online to Virginia's MS program in computer science, and had my recommendations provided online. When I had yet to hear an admissions decision by early April, I called the department to find out when I could expect to know. I was informed that my application had not been evaluated because the paper file on which the admissions committee was basing its decisions seemed to be incomplete; it was missing one of the three required recommendations.

I was very confused by this, as I'd been using the online application system to track and confirm the successful arrival of all of my application materials. To my knowledge, everything was in order, and had been for quite some time. The recommendation thought to be missing had been submitted in mid-November. I pointed this out, and the "missing"

recommendation was promptly found and added to the paper file, but by then the damage was done. Notices were already out to accepted applicants; the best that could be done for me was placement on the waitlist.

What are the risks here? Generating paper applications from online may introduce errors, errors that will not be visible to the applicant. If these paper files are treated as authoritative -- if the online application is not consulted in the case of seeming incompleteness or inconsistency -- applications may be passed over for no good reason at all.

✶ Paypal Meets the Patriot Act

"Hanah Metchis" <hmetchis@cei.org>
Mon, 14 Apr 2003 14:35:01 -0400

CEI C:\SPIN [Excerpted by PGN]

Paypal Meets the Patriot Act, by Solveig Singleton, Senior Policy Analyst

<http://www.cei.org/dyn/view_bio.cfm/163> ,
Project on Technology and Innovation, CEI <<http://www.cei.org/>>
14 Apr 2003.

Paypal has been in the news lately. In this case, a Missouri prosecutor sent eBay a letter

<<http://news.findlaw.com/news/s/20030401/techebaypaypaldc.html>>
insisting that its recent acquisition, Paypal, was violating the Patriot Act

<<http://www.epic.org/privacy/terrorism/hr3162.html>>
by processing payments from Internet gambling operations.

Internet gambling
is illegal in the U.S., but about 5 million Americans use
overseas sites;
eBay discontinued Paypal's gambling operations last fall. This
comes on top
of troubles Paypal has had with the New York attorney general
<<http://www.auctionbytes.com/pages/abn/y02/m08/i22/s01>> and
authorities in
other states. So what's up with Paypal? Is something sinister
going on
there? Far from it. Prosecutors may get paid by the public, but
they don't
always serve the public. [...]

C:\SPIN is produced by the Competitive Enterprise Institute.

⚡ Risks of *not* being lost

David Lesher <wb8foz@nrk.com>
Mon, 31 Mar 2003 10:59:17 -0500 (EST)

Seems many of the ""embedded"" media procured Thuraya brand sat/
cell phones
before departing. These are controlled by a ground station in
Abu Dhabi, and
to optimize performance, the phone locates itself with an on-
board GPS and
reports back that position to the ground station.

Ooops, current exact location is one thing the US does NOT want
the Other
Guys to know. While you could in theory use triangulation or
other schemes
to locate any EM emitter, including a phone, making it easy for
Them is
hardly ever a good idea. The military has confiscated the phones.
The competitor, Iridium, may well also do this too, but

allegedly the GPS reporting can be turned off [how? hardware orsoftware?] and in any case, that ground station is in the US. Given that Iridium is running at all only because Uncle Sam bought a govt-wide license, one could hope that someone has considered the integrity of that aspect beforehand.

Note that the FBI is mandating tracking of all domestic cell phones as well, with the already past due-date being slipped back time and again. Security at our myriad providers can not help but be worse than at that single Iridium ground station.

And in both TV and real life, cops and FBI agents carry cell phones. In the future will oh, Willy Sutton | John Brown | Jonathan Pollard | Paul Reubens be able to track the FBI agents tracking them?

Risk: Be careful what you wish for; most swords do have two sides.

🔥 Nova Scotia police track suspect with GPS

M Taylor <mctaylor@privacy.nb.ca>

Tue, 15 Apr 2003 18:36:04 +0100

Police in Nova Scotia use the On Star system, a GPS based service included in the car to locate the car within minutes of contacting On Star operators in United States. [Source: *Globe and Mail*, 15 Apr 2003]
http://www.globeandmail.com/servlet/RTGAMArticleHTMLTemplate?tf=RT/fullstory_print.html&slug=gtbeatapr15&date=20030415

It is nice to know that occasionally technology increases risk of getting caught to criminals. M Taylor <http://www.mctaylor.com/>

✶ "Quick Deposit" systems

Gervase Markham <gerv@gerv.net>
Mon, 31 Mar 2003 16:13:00 +0100

I wandered into my branch of Barclays Bank in Enfield, UK, this afternoon in order to deposit a couple of cheques. For quite a while, Barclays has had a "Quick Deposit" machine - obviously old tech, green text on a character-mapped screen, no buttons; you just insert your envelope with the cheques and a deposit slip, and it prints a receipt.

Recently, an additional machine of a newer design has been installed. This one looks much more like a cashpoint - number keypad, buttons on the side of the screen - and has card slots, cheque slots, and all sorts of attachments. It's far harder to use and takes much more time than the original. But its UI flaws are for another mailing list.

This afternoon I walked up to it, and noticed that the screen said "NTDetect 4.00". I watched in amazement as the NT 4 boot sequence proceeded, via the "Press Space for Last Known Good menu" (unfortunately, pressing of keys only revealed that none were mapped to Space), the Blue Screen of Bootup (NT4 SP6, 128MB RAM), and the splash

screen ("with Internet Explorer"), to an NT 4 desktop, complete with "Outlook Express" icon!

Some startup scripts ran, which showed me that I was logged in as Administrator, and then some sort of debugging application popped up.

Because it left me in a text input window in this debugging app, I was able to work out the key mappings of the built-in keypad. The number keys produced numbers, Cancel was Backspace and Enter was return. The other keypad keys seemed to have little effect.

Pressing the keys on the side of the monitor seemed to trigger something, because several bits of attached machinery began whirring.

Shame it's not a cashpoint, I thought. I didn't try feeding bits of paper into it. Other sundry error dialogs and DOS boxes gave me some idea of the filesystem layout, running software and so on.

After a couple of minutes, the scripts must have finished, because the desktop disappeared to be replaced with "This Terminal is not in use" in Barclays livery.

The RISKS are many:

- Using a general-purpose OS for an embedded application
- Having the input and output devices connected before the embedded app is ready to accept input
- Using an Administrator account to run your app
- Mapping keys to their obvious equivalents (Return is dangerous; mapping "Enter" to e.g. "G" would have been safer)
- Keeping debugging applications installed on production machines, and having them automatically invoked

✦ Double-barrelled surname costs disabled mother

Nigel Metheringham <Nigel.Metheringham@pobox.com>

14 Apr 2003 10:54:08 +0100

A disabled mother of three has been barred from receiving tax credits

worth 190 pounds a week because she is among hundreds of claimants whose

double-barrel surnames are not recognised by Government computers. Sue

Evan-Jones has fought for more than three months to persuade the Inland

Revenue that her surname has two parts after she was told the system was

confused by hyphens.

The fact that obvious input validation problems, and properly specifying the valid forms of input in the original design are still being got horribly wrong in 2003 fills me with despair.

Source:

<http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2003/04/14/ncred14.xml>

✦ New comprehensive Federal rules on privacy of medical information

Jack Goldberg <jackgoldberg@earthlink.net>

Sat, 12 Apr 2003 22:59:51 -0700

The article in the 12 Apr 2003 *San Jose Mercury News*

<http://www.bayarea.com/mld/mercurynews/news/5614657.htm>

is an easy to read summary of the new Federal rules on privacy of medical information privacy, just being put into effect. There is a very large body of literature on the general subject and on the development of the standards, and the set of rules itself is a huge body of text. This reader sees lots of good intentions, but also lots of problems, such as how medical and computer personnel -- and citizens, can understand the complex rules to determine what is allowed and what is not, how to help a client know whether exercising an option is a good idea or not, whether implementation of the rules will be an intolerable burden on health care practice, and how the integrity of a given implementation can be verified and preserved. On the last point, there seems to be no provision in the law for certification; rather it seems that it will be up to the courts to decide if the rules were violated in a particular case. This development deserves attention.

75+ Organizations urge FBI NCIC database accuracy

Marc Rotenberg <rotenberg@epic.org>

Tue, 8 Apr 2003 12:34:55 -0400

A broad coalition of organizations across the United States has endorsed a letter urging the reestablishment of accuracy requirements for the FBI's National Crime Information Center (NCIC), the nation's largest

criminal
justice database.

More than 3,000 individuals from 47 states and the District of Columbia have signed an online petition to the Office of Management and Budget (OMB) also supporting the Privacy Act accuracy requirements.

The petition drive will continue until the OMB acts on the request.

Individuals may sign the petition online at:

<http://www.petitiononline.com/ncic/petition.html>

[Excerpted for RISKS. See [RISKS-22.65](#) and [22.67](#) for items on the termination of the NCIC accuracy requirements. PGN]

✶ Re: POW Social Security numbers revealed (Hirose, RISK-22.67)

Crispin Cowan <crispin@wirex.com>

Fri, 04 Apr 2003 19:32:26 -0800

It is often suggested that disclosure of SSN's is a great risk. In the current climate, where SSN's are used to *authenticate* an individual ("tell us your SSN so we know it is you") that certainly is true.

However, I suggest an alternate approach to solving the problem of identity theft. SSN's are hopelessly easy to obtain; attempting to curtail the broadcast of these numbers (e.g. hoping the Iraqi state television will control the release) is futile. Instead, I suggest that the US Government

prohibit the use of SSN's as authenticators. If all of the US organizations that currently authenticate with SSN's were forced to use something else (anything else) the state of the identity theft crisis would improve drastically.

The "*anything* else" part is important to this proposal. It is tempting to propose something prescriptive, specifying how organizations should authenticate people. However, I suspect that such prescriptions would make the law founder on impracticality, as organizations find high quality authentication difficult to implement for one reason or another.

In contrast, simply forcing organizations to choose something else at least has the scattershot effect that they are unlikely to choose all the same attributes, making wholesale identity theft much more difficult.

Just me proposing this idea here and getting a few folks to agree that it would be beneficial is fun & all :-) but won't actually change anything. More constructive would be if those who do agree with the idea, and have more influence in the financial regulation space than I do, would take up the idea and start spreading it around.

Crispin Cowan, Chief Scientist, WireX
<http://wirex.com> <http://wirex.com/~crispin/>

✶ Re: The reality behind these laws (Re: Shalunov, [RISKS-22.68](#))

Bill Gunshannon <bill@cs.scranton.edu>

Sun, 13 Apr 2003 09:21:39 -0400 (EDT)

Assuming that the failure of one of the postulates results in the failure of the premise, we can put this one to bed.

Since when is a NAT box "intended to conceal the actual origin of IP traffic"? The intended purpose of NAT and the use it is put to in every case I am aware of is to allow persons with a single IP Address to have more than one host on their network that can all access the INTERNET and I am certain that is the reason LinkSYS gives for selling the products that have NAT built in. On top of that, NAT hides nothing. You still need at least one valid routable IP address and that address is traceable to a fixed location and person responsible.

If the purpose of NAT were to "conceal the actual origin of IP traffic", what then of DHCP?

The RISK here is that we start chasing after demons that don't exist while missing the ones that really do.

Bill Gunshannon, University of Scranton, Scranton, Pennsylvania

✉ Re: Millennium trains taken off the tracks (Colville, [RISKS-22.68](#))

"Bob Frankston" <bob2@bobf.frankston.com>
Sat, 12 Apr 2003 23:31:09 -0400

"Train signals interfering with the frequency of the underground signalling system ... turning lights red for all following trains."

I can't help but wonder what kind of signaling system was being used. This seems to be an ancient analog system that uses the frequency as part of the message rather than a digital signal that has some independence from the path and would have some resilience. Turning a signal red in the absence of other information is understandable but why is the signal so fragile?

I might not have commented were it not for the name "Millennium" train which would indicate a design that reflects today's understanding of signaling. Instead this seems to rely on old techniques such as the use of pristine frequencies because that's the only technique we knew a century ago.

✉ Re: Friendly Fire ([RISKS-22.65](#) to [22.68](#))

"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>
Mon, 14 Apr 2003 13:52:48 +0200

In [RISKS-22.68](#), I gave some figures from [1, Figure 1.1, p1-2] suggesting that the number of fratricide incidents in recent conflicts (from WW II) lay around 1% of casualties. The figure for Desert Storm/Shield that I gave was mistaken. The figures from FM 100-14 Figure 1.1 are:

	World War II	Korea	Vietnam	Desert
Storm/Shield	(1942-45)	(1950-53)	(1965-72)	
(1990-1991)				
Accidents	56%	44%	54%	75%
Friendly Fire	1%	1%	1%	5%
Enemy Actions	43%	55%	45%	20%

Paul Marks of the *New Scientist* pointed out to me that the UK National Audit Office takes a different view. It says that "American research shows that, historically, fratricide accounts for between ten and 15 per cent of friendly casualties during operations." [2, paragraph 1.5]

FM 100-14 speaks simply of "losses". The UK NAO defines fratricide as "destruction of friendly or allied forces". It is possible that these are two different concepts. But it is also possible that people aren't counting very precisely. It's a shame that one cannot tell from either of these documents what the figures actually represent.

[1] U.S. Army Field Manual 100-14, Risk Management, 23 April 1998, available from <http://www.irwin.army.mil/g3/tacticalsafety.html>

[2] National Audit Office, UK, Combat Identification, Report by the Comptroller and Auditor General, HC661 Session 2001-2002: 7 March 2002, available from <http://www.nao.gov.uk/pn/01-02/0102661.htm>

Peter Ladkin, University of Bielefeld, Germany <http://www.rvs.uni-bielefeld.de>

✶ Re: Friendly Fire (Van Meter, [RISKS-22.68](#))

Allan Goodall <agoodall@att.net>

Mon, 14 Apr 2003 14:50:41 -0500

Mr. Van Meter explains that the term "casualty" refers to persons "killed or injured". This is not correct. Casualties refer to persons killed, injured, or *missing*.

"Missing" includes anyone whose whereabouts are unknown. The soldier may have been captured by the enemy, or they may have run away to -- possibly -- turn up later, or they may have been killed but their remains hadn't been identified or their remains were unidentifiable.

I agree with Mr. Van Meter that confusion over the term "casualty" has caused much misinformation. In September 2002, on the 140th anniversary of the American Civil War battle of Antietam (the single bloodiest day in American history), CNN Headline News mentioned that there were 23,000 men killed in the battle. The total casualties were just less than 23,000, 3600 of whom were killed (though many of the 1700 missing men were likely dead and buried in unmarked graves, and many of the wounded would die sometime later). This error is particularly ironic as Ted Turner is a Civil War buff.

Allan Goodall agoodall@hyperbear.com <http://www.hyperbear.com>

✶ Changing Domain Registration info without verification

<risks@Orwellian.Org>

Sun, 30 Mar 2003 16:41:51 -0500

I found a reference to a USPS Web site allowing anyone to issue a change of address via the web in a 1997 issue of RISKS.

[Actually, it allowed you to print a form that you could mail in.

See [RISKS-19.18](#) to [19.20](#). PGN]

Here's a twist I recently noticed, as conveyed in a message I just sent

Network Solutions:

I just tried to login to my ***** account for the first time in a long

time, and it is trying to force me to accept a service agreement before I

can access my account.

I don't know if it was in the previous service agreement, but this

provision is UNACCEPTABLE:

4) You agree that VeriSign is authorized, but not obligated, to use Coding Accuracy Support System (CASS) certified software

and/or the National Change of Address program (and/or such other

systems or programs as may be recognized by the United States

Postal Service or other international postal authority for updating and/or standardizing address information) to change any address information associated with your account (e.g., registrant address, billing contact address, etc.), and you agree

that VeriSign may use and rely upon any such changed address information for all purposes in connection with your account (including the sending of invoices and other important account

information) as though such changes had been made directly by you.

This USPS change-of-address can be done BY ANYBODY WITHOUT VERIFICATION at

<https://moversguide.usps.com/>

I DO NOT authorize that my contact information be changeable by anyone via this process. (The USPS site even lets the e-mail address be changed.)

If you cannot remove this clause from my agreement to service, I will transfer my registration to Register.com, which does not have this provision.



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

[ACM](#) Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 70

Sunday 20 April 2003

Contents

- [Turtle triggers search and rescue effort](#)
[Jim Griffith](#)
- [Rules let marketers see patient data](#)
[Monty Solomon](#)
- [Airline boarding pass algorithm flaw](#)
[Mark Kantrowitz](#)
- [CNN glitch reveals premature obits](#)
[NewsScan](#)
- [NASCAR fan faces prison time for flooding Fox with angry e-mails](#)
[Monty Solomon](#)
- [Careless use of Web templates](#)
[Colin Andrew Percival](#)
- [Misusing emergency capabilities](#)
[Kevin C Stevens](#)
- [Cyberstalking on the rise](#)
[NewsScan](#)
- [Online harassment: bogus e-mail incites retribution](#)
[Monty Solomon](#)
- [Qmail-ldap discloses Bcc recipients](#)
[John Pettitt](#)

- [Sony to recall 20,000 more Vaio PCs due to glitch](#)
[Monty Solomon](#)
 - [Y2K bug alive and working for Macdonalds](#)
[Richard A. O'Keefe](#)
 - [Re: POW Social Security numbers revealed](#)
[Markus Kuhn](#)
 - [Re: Millennium trains taken off the tracks](#)
[Ben Low](#)
 - [Re: "Quick Deposit" systems](#)
[Brian Campbell](#)
 - [Re: Friendly Fire](#)
[Mark Brader](#)
 - [Correction on fratricide item](#)
[Peter B. Ladkin](#)
 - [Re: Traffic lights don't work in the snow](#)
[Ed Ravin](#)
 - [Web site wants me to change my proxy? I don't think so...](#)
[Sean Sosik-Hamor](#)
 - [Workshop on Wireless Security WiSe 2003 CFP](#)
[Adrian Perrig](#)
 - [Info on RISKS \(comp.risks\)](#)
-

🚀 Turtle triggers search and rescue effort

Jim Griffith <griffith@dweeb.org>

Fri, 18 Apr 2003 12:51:15 -0400

The U.S. Coast Guard launched a massive search and rescue effort earlier this week after picking up an emergency distress beacon signal. They finally pinpointed the cause - a turtle had become tangled in a rope tied to a discarded beacon. The original owner was located, and he said he'd lost it some time ago.

<http://www.cnn.com/2003/WORLD/americas/04/18/bermuda.turtle.search.ap/index.html>

✶ Rules let marketers see patient data

Monty Solomon <monty@roscom.com>

Sun, 20 Apr 2003 01:25:21 -0400

In an emergency, the hospital can't tell anyone except family that you're a patient. But it's free to use intimate medical details to forward marketing pitches to you from drug companies, insurers, and other "business associates". U.S. Representative Edward J. Markey, Massachusetts Democrat, has filed a bill that would require patient consent. ... [Source: Diane E. Lewis, subtitled Campaign afoot to give patients right to block release of files, *The Boston Globe*, 19 Apr 2003; PGN-ed] http://www.boston.com/dailyglobe2/109/business/Rules_let_marketers_see_patient_data+.shtml

✶ Airline boarding pass algorithm flaw

"Kantrowitz, Mark" <mkant@fastweb.com>

Mon, 7 Apr 2003 19:51:11 -0400

On a recent USAir flight, two people were both assigned to the seat in front of me. It turns out that they both had the exact same name. One was female

and the other male, but their full names were spelled identically.

Both were issued boarding passes for the same seat.

This suggests that the algorithm the airline uses to issue boarding passes is based on the flight number and passenger name, and not based on a unique identifier such as ticket number or passenger id number.

Besides being a potential security risk, I would not be surprised if it costs the airline some lost revenue.

[Perhaps. But it also might be thought of as saving a little in programming complexity and maintenance? On the other hand, you would think there was a flag for "boarding pass already issued". PGN]

Mark Kantrowitz PO Box 81620, Pittsburgh, PA 15217 1-412-422-6190
www.fastweb.com www.finaid.org www.edupass.org www.monster.com

✶ CNN glitch reveals premature obits

"NewsScan" <newsscan@newsscan.com>

Fri, 18 Apr 2003 09:53:43 -0700

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; NewsScan Daily, 18 Apr 2003]

http://news.com.com/2100-1025-997367.html?tag=fd_top

[As I recall, a similar situation happened previously, to *The New York

Times*, but I cannot find the entry in RISKS. PGN]

✶ NASCAR fan faces prison time for flooding Fox with angry e-mails

Monty Solomon <monty@roscom.com>

Thu, 17 Apr 2003 14:21:51 -0400

A NASCAR fan faces up to a year in prison for flooding Fox Entertainment

Group in Los Angeles with more than a half-million e-mails because he was

angry the network aired a Boston Red Sox game instead of an auto race in

early April and May 2001. Michael Melo of Billerica agreed to plead guilty

to a federal misdemeanor charge of damage to a protected computer system,

(Fearing a cyberattack, Fox shut down part of its Web site, and claims it

cost them \$36,000.) [Source: Mark Pratt, Associated Press, 16 Apr 2003.

PGN-ed]

http://www.boston.com/dailynews/106/region/NASCAR_fan_faces_prison_time_f:.shtml

✦ Careless use of Web templates

Colin Andrew Percival <cperciva@sfu.ca>

Mon, 7 Apr 2003 08:26:47 -0700 (PDT)

Most people who use Google routinely will have noticed that many of the "sponsored links" seem to be built from templates; this works reasonably well in most cases, but sometimes fails badly.

While conducting a terrorism-related search, I was confronted with the following advert:

```
Terrorism - Huge Range, Low Prices, Great Service - CLICK HERE!  
www.amazon.co.uk Free Super Saver Delivery on orders over #39  
(see  
conditions)
```

While in this case the only risk was one of unintended humour, it is clear that unforeseen consequences can ensue from allowing too wide a range of terms to be inserted into such a template. Imagine, for example, the possible reactions if "Terrorism" were replaced by "Child Pornography".

✦ Misusing emergency capabilities

Kevin C Stevens <kcs6@cse.Buffalo.EDU>

Sat, 5 Apr 2003 13:20:22 -0500 (EST)

The small liberal-arts college where my wife teaches has an campus-wide alert system. One component of that system is the ability to

make an announcement over a PA system. It is used very rarely and has dubious sound quality. In fact, previous to this week the only two times anyone can remember it being used were for a severe ice storm when the university was about to be closed; and 9/11.

Yesterday, a moderately severe ice storm struck the region (we are in Western New York). There was also a recruiting event for potential new students that evening for which the publicity flyers had the wrong venue. As a consequence, high-school seniors and their parents were going from building to building looking for the event.

You guessed it, they used the campus emergency PA system to make an announcement that those "All those looking for the recruiting event should gather in <name of building omitted> for directions."

The dorms emptied, both because the message was poorly understood and because if it came over the campus PA, it must be critical. So a few hundred college students left their dorms and wandered out on a cold night, some in pajamas, only to find out there was no need to be out.

The RISK is obvious, if it was meant for emergencies, only use it for an emergency.

Kevin Stevens, Department of Computer Science, University of Buffalo, SUNY

✶ Cyberstalking on the rise

"NewsScan" <newsscan@newsscan.com>

Fri, 18 Apr 2003 09:53:43 -0700

Cyberstalking -- stalking people over the Net -- is increasing across the U.S., according to a new study by Wired Safety. And while women remain the most likely targets, they're getting into the act as perpetrators, too. In addition, growing numbers of children are cyberstalking children. "We didn't find much good news," said Wired Safety executive director Parry Aftab. "Identity theft is increasing. And because more people are cyber dating they become victims of cyberstalking when things don't work out." Aftab expressed concern over a recent court ruling that compelled Verizon to turn over the name of an ISP subscriber under the subpoena power of the Digital Millennium Copyright Act. "This is an outrageous and dangerous ruling. It was supposedly about music piracy, but the result of the case is that anyone can obtain personal information about any Internet user by simply filling out a one-page form and submitting it to a court clerk. There is absolutely nothing you can do to protect yourself, even if you are a police officer doing undercover work against s*xual predators. The future safety and privacy of all Americans engaged in online communications now rests with Verizon winning this case on appeal." [Asterisk inserted so that NewsScan Daily doesn't get caught in the software filters meant to ward off pornography.] [Internet News 18 Apr 2003; NewsScan Daily, 18 Apr 2003]

<http://dc.internet.com/news/article.php/2193131>

✶ Online harassment: bogus e-mail incites retribution

Monty Solomon <monty@roscom.com>

Sun, 20 Apr 2003 00:50:28 -0400

Arab-American activist Nawar Shora checked his e-mail one day and found scores of angry messages asking why he hated Americans and Jews. The messages were responding to e-mail messages with his spoofed From: address. However, he had never sent the hate mail; the From: address had been forged [which is easy to do]. [Source: New online harassment involves provocative messages sent under guise of activists, Anick Jesdanun, Associated Press, 18 Apr 2003; PGN-ed]

<http://www.boston.com/dailynews/108/economy/>

[New online harassment involves:.shtml](#)

✶ Qmail-ldap discloses Bcc recipients

John Pettitt <jpp@cloudview.com>

Fri, 11 Apr 2003 08:56:29 -0700

The technique of Bcc'ing all the recipients is often used to send e-mail messages where the nature of the subject matter is controversial with the intent of not disclosing who is interested in the message.

However gmail discloses some of the recipients by listing the first of the bcc'd recipients in a Received by header.

What seems to happen is that the MTA adds a header like this:

```
Received: from 11.22.33.44 (HELO some.domain) ([11.22.33.44])
  by some-other.domain (gmail-ldap-1.03) with SMTP
  for <first.envelope.recipinet@another.domain>;
```

This happens even when there are no To: or Cc: recipients listed.

A trivial search of my mail archive finds many cases where a "for" clause in a received header was neither my address or the address of any of the publicly listed recipients.

So far I've only found this behavior in gmail-ldap and it's not clear if the problem exists beyond the first hop in the delivery chain or in other MTA's.
(My tests on postfix suggest it's not a problem.)

✶ Sony to recall 20,000 more Vaio PCs due to glitch

Monty Solomon <monty@roscom.com>

Sat, 19 Apr 2003 14:27:52 -0400

Consumer electronics giant Sony Corporation said on 18 Apr 2003 that it would recall 20,000 Vaio desktop personal computers sold in Japan between Sep 2002 and Jan 2003, to replace defective power supply parts. This is in addition to 20,000 Vaio PCs recalled in the United States and Canada in Dec 2003 due to a similar problem, a Sony spokesman said. [Source:

Reuters, 18

Apr 2003; PGN-ed]

<http://finance.lycos.com/home/news/story.asp?story=33881151>

✶ Y2K bug alive and working for Macdonalds

"Dr Richard A. O'Keefe" <ok@cs.otago.ac.nz>

Wed, 16 Apr 2003 14:43:47 +1200

Last week my elder daughter had her 7th birthday. The party was held at a local Macdonalds. (NOT my choice.) One of the things they provided was a cake. On the box, there was a use-by date. It was a day in July 1903.

Makes me wonder how many Y2K bugs are still lurking in dark corners.

[This one really takes the cake! PGN]

✶ Re: POW Social Security numbers revealed (Cowan, RISK-22.69)

Markus Kuhn <Markus.Kuhn@cl.cam.ac.uk>

Wed, 16 Apr 2003 18:08:55 +0100

> SSN's are hopelessly easy to obtain

Well, there is a good opportunity to turn a bug into a feature:

The U.S. social security administration could simply make their entire database of social security numbers and associated names and dates of

birth openly available to the general public for download, and of course publicise this step prominently. As a result, the SSN would instantly lose any usefulness whatsoever as an authenticator and become even more harmless and fear-free than telephone numbers or ZIP+4 codes. Problem solved. [I can literally hear a few thousand US RISKS readers breathing in sharply at this idea as they feel cold shivers running down their back, so deeply is the cultural fear of anyone else knowing a few digits associated with you engraved in a nation's collective psyche ... ;-]

Such a step would of course require [listed in order of increasing difficulty]

- (a) some warning time for organizations who currently use the SSN as part of an authentication procedure to give them time to adjust their practices,
- (b) the introduction of a proper authentication mechanism as an alternative,
- (c) a population that can mentally make that step and overcome deeply embedded phobias about the entire idea of other people being able to look up *YOUR* number, no matter how little (ab)usefulness knowledge of that number has in practice

> It is tempting to propose something prescriptive, specifying how organizations should authenticate people. ...

Many countries have done that long ago. They run reasonably carefully

administered population registers and residents are entitled to get a tamper-resistant copy of their entry of that register, to show it to other people whenever establishing identity is desired in a transaction.

These tamper-resistant copies are usually "called ID" cards, or, where the form factor is a somewhat larger booklet with sufficient space for travel visas, they are called "passports". In those few (typically anglophone) countries where the term "ID card" causes shivers running down the back of too many scared people for cultural reasons, the same thing is now called "entitlement card" or "driver's licence".

Passports and ID cards are widely considered the only accepted serious form of authentication in continental Europe. At first sight, they seem to be only useful for card-holder present transactions, e.g., were you physically walk into a bank, school, administration, etc. However, that does not mean that they are useless for using online services from home. It is not too difficult to build remotely usable proper authentication mechanisms on top of ID cards. For example, on top of a well-run ID card infrastructure, it becomes immediately feasible for the national postal service to offer authenticated personal delivery. For a small additional fee, a package or letter sent to you will only be handed over to you if you show up personally in the nearest post office and authenticate yourself with your ID card, which contains all the information that allows the postal office clerk to verify that your biometrics belong to the person named as the

recipient of the letter. Once you have authenticated postal delivery, companies can easily send all sorts of authentication tools to you, such as lists of transaction numbers, floppy disks or chips with certified crypto keys, etc.

Banks and delivery services might find it an attractive business opportunity to offer similar authenticated delivery services. By using two independent routes to deliver electronic authenticators to you (two shares of a secret key arrive via postal authenticated delivery and via pickup from your local bank branch), abuse of the system by malicious employees in the delivery chain can be made unattractive enough for potential fraudsters to look elsewhere for work.

Governments setting up the underlying ID infrastructure remains a prerequisite for all these more convenient and safer forms of authentication to become available.

Markus Kuhn, University of Cambridge, GB <http://www.cl.cam.ac.uk/~mgk25/>

✦ Re: Millennium trains taken off the tracks (Frankston, [RISKS-22.69](#))

Ben Low <ben@bdlow.net>
Sat, 19 Apr 2003 01:38:59 +1000

The interference caused by the Millennium trains may simply be trashing the

signal completely, possibly across a wide range of frequencies.
In which
case, as noted, the fail-safe for all listening devices would
surely be "go
to red".

Indeed, if it were an analogue system, you'd expect the quote to
be "turning
lights red, green or orange for all following and leading
trains" :-)

(BTW, I suspect the original quote meant "interfering *on* the
frequency of
the ... signalling system", rather than *with* the frequency. :-)

✉ Re: "Quick Deposit" systems

Brian Campbell <bacam@z273.org.uk>

Sat, 19 Apr 2003 15:31:09 +0100

In [Risks 22.69](#), Gervase Markham described a ATM-like deposit
machine booting
Windows NT and allowing a little control with the provided
keypad and
buttons before displaying a "not in use" message. He summarised
[various
risks,] but I don't think these really capture the nature of the
problem.
Essentially, the interface presented to the end-user is wider
than intended,
exposing implementation details and associated risks.

When engineering systems a key method of improving reliability
and security
is to reduce complexity. Providing the software with a normal
keyboard
interface for the keypad makes a lot of sense for reduced
complexity.

Similarly, keeping some of the debugging tools around is often helpful for diagnosing faults.

As such, it would be better if the system restricted the built-in keys and display to the actual application, and have internal connections for attaching a second keyboard and display which act as normal for use when debugging. However, this does require that the operating system support using multiple keyboards and displays separately.

✂ Re: Friendly Fire (Goodall, [RISKS-22.69](#))

Mark Brader <msb@vex.net>
Wed, 16 Apr 2003 00:11:17 -0400 (EDT)

I'm reminded of the way that many people writing about the Titanic disaster tend to assert that about 1,520 *passengers* were killed. Actually it was 820 passengers and 700 crew, out of 1320 and 900 respectively, all this in round numbers. Note that the crew death rate was significantly higher.

✂ Correction on fratricide item (Ladkin, [RISKS-22.68](#))

"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>
Mon, 14 Apr 2003 13:49:02 +0200

Im my fratricide note in [RISKS-22.68](#), I gave figures from FM 100-

14 via

Chris Johnson that the fratricide figure for Desert Storm/Shield was 1%

according to FM 100-14. Well, FM 100-14 in fact says 5% for Desert

Storm/Shield fratricide (I found an on-line copy). All the other figures in

the table in my note are correctly transcribed from FM 100-14.

[Annotated correction is being made in the official archives. PGN]

In my new note, I give on-line source for FM 100-14, and also quote a UK

National Audit Office report that says that US research has shown that

historically the figure lies around 10-15%, not the 1-5% that FM 100-14

says.

Peter B. Ladkin, Professor of Computer Networks and Distributed Systems,

Faculty of Technology, University of Bielefeld, 33594 Bielefeld, Germany

⚡ Re: Traffic lights don't work in the snow ([RISKS-22.65](#))

<Ed Ravin <eravin@panix.com>

Tue, 1 Apr 2003 00:25:45 -0500 (EST)

For those of us who ride bicycles, we've been dealing with this problem ever

since the technology was introduced. Sometimes lying your bicycle on the

ground over the sensor is enough to trigger it. Other options are to look

for a button meant for use by pedestrians, to wait for a motor vehicle to

show up and trigger the sensor, and finally, the most popular option in my observation, merge with traffic as best one can regardless of the state of the traffic signal.

I'm told most of these devices can be tuned to sense bicycles, but traffic engineers in the U.S. are notorious for taking the "windshield view" - that is, they see everything on the road from the perspective of a driver in a motor vehicle. It's a classic case of building a system for 99% of the users and making life miserable for the other 1%.

> You have no choice but to attempt to join a potentially busy road by going
> through a red light or ride on the pavement to a safe spot to rejoin
> traffic.

To clarify for our American readers, I believe what Ryan calls "riding on the pavement" would be "driving on the sidewalk" in Americanese, or "operating a motor vehicle on the pedestrian right-of-way" in bureaucratese.

🔥 Web site wants me to change my proxy? I don't think so...

Sean Sosik-Hamor <ssh@mac.com>
Mon, 31 Mar 2003 11:13:24 -0500

It appears that OnlineNIC, a discount bulk domain registrar that caters to domain squatters, has been attacked and their Web servers are unavailable. We had to deal with them about a year ago to transfer a domain

name away

from a squatter in Korea and found their customer support extremely lacking.

On top of that, even after successfully transferring the domain name away

from them, they seem to think that we're still a customer so we keep

receiving promotional and maintenance e-mail from them.

I received the following maintenance e-mail from them this morning informing

me that their servers are under attack. It is unclear whether the attack is

simply a denial of service attack or if their Web servers were actually

compromised. Regardless, the request that OnlineNIC has made in the

following e-mail is absolutely outrageous. After informing me that their Web

servers are under attack (I didn't trust them before and I sure don't trust

them now that I know they may have been compromised), they want me to change

my proxies to one of theirs.

To quote many RISKS posters that came before me, the RISKS here are obvious.

If this request is legitimate due to a denial of service attack then I would

assume that they are filtering out all traffic to their Web servers and only

allowing traffic to their Web server from their proxies. In theory, I'm

sure this idea made sense to someone somewhere in the OnlineNIC chain of

command. Regardless, setting my proxy to one of theirs would send all my

Web traffic through it...not just traffic to OnlineNIC. I really don't

think I trust OnlineNIC with logs and caching of every Web site I visit.

Since I'm a paranoid freak, I'm assuming that OnlineNIC's Web servers were completely compromised (my theory, no way to confirm), their customer base was leaked, the attacker sent this e-mail to all customers and the below proxies are hostile and designed specifically to log all Web traffic for OnlineNIC's customers. I only come to this conclusion because the headers of this e-mail are very sparse and seem forged (Received from: YOURNAME localhost.localdomain), there are typos in the e-mail and the e-mail asks me for my username/password.

Oh well...even if the request was legitimate, how many naive users who actually switch their proxies are going to remember to switch them back after OnlineNIC comes back online? If the proxies are no longer required, how long with OnlineNIC keep those proxies online for the "convenience" of their customers? And, are these proxies wide open for anyone to use for semi-anonymous surfing? If the request is legitimate, OnlineNIC is opening themselves up to abuse by making these proxies available.

/Sean/

Begin forwarded message:

> From: "support@onlinenic.com"<support@onlinenic.com>
> Date: Mon Mar 31, 2003 5:42:49 AM US/Eastern
> To: foo@bar.com
> Subject: About the problem of Onlinenic
>
> Dear Customer,
>
> We are sorry to inform you that our WEB server has been attacked by

> somebody. Our technicians are taking great effort in getting
it
> solved now. Please rest assured that the problem will be
solved soon.
>
> To visit Onlinenic, would you please try it at
> <https://www.onlinenic.com>, if it still fails, please try to
use the
> proxy server: 218.104.136.170:80 in the following way:
>
> Go to 'Tools' in IE, choose 'Internet' , it will lead you to an
> interface, then choose 'Connect', click 'LAN setup', then you
may set
> up the proxy 218.104.136.170 with the port 80.
>
> If this proxy server doesn't work, you may try the following
ones:
>
> 202.239.161.7:80
> 202.30.243.63:80
> 211.140.27.146:80
> 211.141.95.112:80
> 211.141.95.122:80
> 211.141.95.88:80
> 211.141.95.90:80
> 211.141.95.91:80
> 212.141.54.32:80
>
>
> Plus, Some of the e-mail sent to support@onlinenic.com may
have lost.
> If you haven't got any reply from us, please write to
> support@onlinenic.net. Please rest assured that we will never
ignore
> any e-mail reaching us.
>
> If you have domains which are supposed to be registered
urgently,
> please kindly offer us your id, password and the detailed whois
> information of your domains, we will try to help you register
them
> here.
>

> Please rest assured that you may feel free to change your
account
> password after the domains have been registered successfully
here for
> you.
>
> Your kind understanding and cooperation will be highly
appreciated.
>
> Should you have further questions, please feel free to contact
us.
>
> Sincerely,
>
> OnlineNIC Customer Care
>
> E-mail: support@onlinenic.com
> <https://www.OnlineNIC.com>

✶ Workshop on Wireless Security WiSe 2003 CFP

Adrian Perrig <adrian@ece.cmu.edu>
Tue, 15 Apr 2003 20:16:09 -0400 (EDT)

Call for Papers

Workshop on Wireless Security (WiSe) in conjunction with ACM
MobiCom 2003

Sponsored by SIGMOBILE

19 Sep 2003, San Diego, CA

<http://www.ece.cmu.edu/~adrian/wise2003>

[PGN-excerpted for RISKS. See full call for papers:]

<http://www.ece.cmu.edu/~adrian/wise2003/cfp.txt>

The workshop on Wireless Security will be held in conjunction
with ACM
MobiCom 2003. The objective of this workshop is to bring
together

researchers from research communities in wireless networking, security, applied cryptography, and dependability; with the goal of fostering interaction. With the proliferation of wireless networks, issues related to secure and dependable operation of such networks are gaining importance.

Topics of interest include, but are not limited to:

- * Key management in wireless/mobile environments
- * Trust establishment
- * Intrusion detection, detection of malicious behaviour
- * Revocation of malicious parties
- * Secure PHY/MAC/routing protocols
- * Secure location determination
- * Denial of service
- * User privacy
- * Anonymity, prevention of traffic analysis
- * Dependable wireless networking
- * Monitoring and surveillance

Instructions for electronic submission of papers will be posted at

<http://www.ece.cmu.edu/~adrian/wise2003/submission.html>

Paper submissions due: May 27, 2003

Workshop Co-Chairs:

- * Douglas Maughan, DARPA (dmaughan@darpa.mil)
- * Adrian Perrig, Carnegie Mellon University (perrig@cmu.edu)



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

[ACM](#) Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 71

Saturday 3 May 2003

Contents

- [OpenBSD release protects against buffer-overflow attacks](#)
[SANS via Monty Solomon](#)
- [Prescription error](#)
[Monty Solomon](#)
- [Spelling checker renames Amritsar to AmriCzar](#)
[David J. Aronson](#)
- [Kellogg's American Airlines online sweepstakes swept away](#)
[PGN](#)
- [Pilots fail exams](#)
[Jill Treu](#)
- [Inside Cisco's eavesdropping apparatus](#)
[Declan McCullagh via Monty Solomon](#)
- [Internet fraud complaints triple](#)
[NewsScan](#)
- [Bogus Internet domain-name renewal offers](#)
[Network Solutions via PGN](#)
- [Spammers use viruses to hijack computers](#)
[NewsScan](#)
- [Breastfeeding mothers, avoid Continental](#)
[Meng Weng Wong via Dave Farber](#)

- [Re: NCIC database accuracy requirements](#)
[John Beattie](#)
 - [Re: Friendly Fire](#)
[Jan C. Vorbrueggen](#)
 - [REVIEW: "Firewalls and Internet Security", Cheswick/Bellovin/Rubin](#)
[Rob Slade](#)
 - [REVIEW: "Inside the Security Mind", Kevin Day](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✂ OpenBSD release protects against buffer-overflow attacks (SANS)

Monty Solomon <monty@roscom.com>
Sun, 20 Apr 2003 22:28:52 -0400

Excerpt from
SANS NewsBites April 16, 2003 Vol. 5, Num. 15
http://www.sans.org/newsletters/newsbites/vol5_15.php

The most recent release of OpenBSD should eliminate buffer overflows, according to the group's project leader. The group took three approaches to hardening the software. First, the location of the stack in memory is randomized. Second, the team added a tag to the memory structure that will detect address modifications. Finally, they managed to divide the main memory into two sections: writable and executable; the pieces of data and programs, called "pages", would be stored in one or the other section, ensuring that no page is writable and executable at the same time.

<http://news.com.com/2100-1002-996584.html>

[Editor's Note (Gene Schultz): Many kudos are in order here. If what the OpenBSD people are doing really works, they will put considerable pressure on other vendors and developers to do the same. Buffer overflow problems continue to plague operating systems and applications. Eliminating this category of vulnerabilities would be a major victory for the information security arena.

(Schneier): It's great to see this kind of approach to buffer overflows. This is an example of building in security instead of trying to patch it afterwards.

(Ranum): It's GREAT to see that at least a few people are smart enough to try to attack problems like this systemically, rather than keeping stuck in the fruitless "penetrate and patch" while loop. This is how to make progress in security: fundamental protections.

(Shpantzer): Initiatives like this should be taught as case studies in computer science courses at the undergraduate level.
]

⚡ Prescription error

Monty Solomon <monty@roscom.com>
Tue, 8 Apr 2003 02:57:07 -0400

I recently had a prescription filled that was written for 60 pills with 4 refills. The pharmacist made a data-entry mistake, and the

prescription was
entered for 60 pills with 60 refills!

Because prescriptions are valid for a year, the pharmacy computer could have detected the error and alerted the pharmacist. But, in this case, the prescription was printed by my doctor's computer so the issue of reading the doctor's handwriting was not an issue.

The pharmacist may be used to finding the number of refills in a specific place on the prescription and the computer generated prescription might have the number of refills and quantity of pills in unusual places. The prescription was laser printed in the corner of a standard 8.5" x 11" piece of paper so the form factor of the prescription was also non-standard.

[I suppose Monty was lucky the fields were not transposed. Imagine having a prescription for 60 refills of 4 pills each. PGN]

✶ Spelling checker renames Amritsar to AmriCzar

"David J. Aronson" <postmaster@airmsun.dcfido.org>
Tue, 29 Apr 2003 11:53:15 -0400

A Reuters news story written yesterday ("Revenge Behind Air India Bombing, Court Told", by Allan Dowd) included mention of "the Golden Temple in the city of AmriCzar". Google-ing AmriCzar revealed eight hits, compared to the about 141,000 of the correct spelling. (That, as you may have

guessed, is Amritsar.) The six shown (two other similar hits were omitted) are:

<http://www.washingtonpost.com/wp-dyn/articles/A58594-2003Mar7.html>

<http://www.punjabi.net/talk/messages/1/829.html>

<http://cndyorks.gn.apc.org/news/articles/asia/itemsonconflict.htm>

<http://terrorism.com/>

<http://www.ocf.berkeley.edu/~andychou/archive200211.htm>

http://www.jekyl.com/jekyl/arc_Nov02.htm

(Note that some of these are quoting Reuters articles!)

At a guess, the cause seems to have been blind string-matching without regard for context, including whether the string was part of a larger word.

The RISK? Fortunately, just mild embarrassment in this case, and even that is assuming that the IT folks at Reuters ever catch wind of this. However, we've seen worse consequences reported here before due to similar "help", even when the "correction" is limited to spelling....

David J. Aronson, Software Engineer for hire in Washington DC area.

See <http://destined.to/program/> for online resume, references, etc.

[Roto-reuters strike again. PGN]

⚡ Kellogg's American Airlines online sweepstakes swept away

"Peter G. Neumann" <neumann@csl.sri.com>

Wed, 30 Apr 2003 16:07:58 PDT

The Kellogg Company ("cereal giant") began a two-month sweepstake intended to give away one grand prize of 25,000 American Airlines' AAdvantage miles each day for 60 days. Unfortunately, due to a "computer glitch", several thousand people were erroneously notified by e-mail that they were winners -- and then later notified that the earlier e-mail was in error but that they would receive 500 miles as a goodwill gesture. [Source: AP item, 29 Apr 2003; PGN-ed]
<http://www.siliconvalley.com/mld/siliconvalley/>

✶ Pilots fail exams

"Treu, Jill" <Jill.Treu@compuware.com>
Wed, 23 Apr 2003 11:10:42 -0400

[For those readers who wonder about why this item is relevant to RISKS, please remember that technology usually depends on a lot of people. PGN]

The pilots couldn't pass the psychological and physical tests to be allowed to carry a firearm --- but flying huge planes full of people is OK. Oh, this makes so much sense! The risks should be obvious.

Four pilots did not finish gun training. Four of the 48 veteran airline pilots who began the government's first training course for pilots wishing to carry guns in the cockpit were rejected after they failed

at least one

of the battery of required background checks, psychological exams and

firearms tests. Officials said the four rejections showed that the

government was serious about providing guns only to pilots who were

psychologically and physically fit to carry firearms in flight and defend

their planes against attackers. The bill permitting airline pilots to

carry guns was passed by Congress last year, a legacy of the hijackings on

11 Sep 2001, over the serious objections of senior members of the Bush

administration and some members of Congress. [Source: *The New York

Times*, 22 Apr 2003]

<http://www.nytimes.com/2003/04/22/international/worldspecial/22PILO.html>

✶ Inside Cisco's eavesdropping apparatus (from Declan McCullagh)

Monty Solomon <monty@roscom.com>

Tue, 22 Apr 2003 02:26:16 -0400

By Declan McCullagh, 21 Apr 2003

Cisco Systems has created a more efficient and targeted way for police and

intelligence agencies to eavesdrop on people whose Internet service provider

uses their company's routers.

The company recently published a proposal that describes how it plans to

embed "lawful interception" capability into its products. Among

the
highlights: Eavesdropping "must be undetectable," and multiple
apolice
agencies conducting simultaneous wiretaps must not learn of one
another. If
an Internet provider uses encryption to preserve its customers'
privacy and
has access to the encryption keys, it must turn over the
intercepted
communications to police in a descrambled form.

Cisco's decision to begin offering "lawful interception"
capability as an
option to its customers could turn out to be either good or bad
news for
privacy.

Because Cisco's routers currently aren't designed to target an
individual,
it's easy for an Internet service provider (ISP) to comply with
a police
request today by turning over all the traffic that flows through
a router or
switch. Cisco's "lawful interception" capability thus might help
limit the
amount of data that gets scooped up in the process.

On the other hand, the argument that it hinders privacy goes
like this: By
making wiretapping more efficient, Cisco will permit governments
in other
countries -- where court oversight of police eavesdropping is
even more
limited than in the United States -- snoop on far more
communications than
they could have otherwise.

Marc Rotenberg, head of the Electronic Privacy Information
Center, says: "I
don't see why the technical community should hardwire
surveillance standards
and not also hardwire accountability standards like audit logs
and public

reporting. The laws that permit 'lawful interception' typically incorporate both components -- the (interception) authority and the means of oversight -- but the (Cisco) implementation seems to have only the surveillance component. That is no guarantee that the authority will be used in a 'lawful' manner."

U.S. history provides many examples of government and police agencies conducting illegal wiretaps. The FBI unlawfully spied on Eleanor Roosevelt, Martin Luther King Jr., feminists, gay rights leaders and Catholic priests. During its dark days, the bureau used secret files and hidden microphones to blackmail the Kennedy brothers, sway the Supreme Court and influence presidential elections. Cisco's Internet draft may be titled "lawful interception," but there's no guarantee that the capability will always be used legally.

Still, if you don't like Cisco's decision, remember that they're not the ones doing the snooping. Cisco is responding to its customers' requests, and if they don't, other hardware vendors will.

If you're looking for someone to blame, consider Attorney General John Ashcroft, who asked for and received sweeping surveillance powers in the USA Patriot Act, along with your elected representatives in Congress, who gave those powers to him with virtually no debate.

I talked with Fred Baker, a Cisco fellow and former chairman of the Internet Engineering Task Force (IETF), about his work on the "lawful interception"

draft. ...

<http://news.com.com/2010-1071-997528.html>

Internet fraud complaints triple

"NewsScan" <newsscan@newsscan.com>

Thu, 10 Apr 2003 08:15:43 -0700

Complaints about fraudulent schemes perpetrated over the Internet tripled in 2002 from the previous year, with the most common grievance being auction fraud, followed by non-delivery of promised merchandise, credit card fraud and fake investments. According to a report from the Internet Fraud Complaint Center, which is run by the FBI and the National White Collar Crime Center, the 48,252 complaints referred for prosecution in 2002 represent only a fraction of the crimes authorities believe are occurring. The center also received almost 37,000 other complaints that did not constitute fraud, but involved such things as spam, illegal child pornography and computer intrusions. The report says 80% of known fraud perpetrators and about 71% of complainants are male. Fraud complaints originated in all parts of the country, with a third coming from California, Florida, Texas and New York. One of the most persistent scams described in the report is the infamous "Nigerian letter," which urges victims to pay an upfront fee (characterized as a bribe to the government) in order to receive

non-existent funds from the "Government of Nigeria." There were 16,000

complaints related to that scam in 2002, up from 2,600 in 2001.

[AP, 9 Apr

2003; NewsScan Daily, 10 Apr 2003]

<http://apnews.excite.com/article/20030409/D7QA6UFO0.html>

✶ Bogus Internet domain-name renewal offers

<neumann@csl.sri.com>

Wed 23 Apr 2003

The following CUSTOMER SERVICE ANNOUNCEMENT warns of bogus e-mail offering domain renewals.

> Date: Tue, 22 Apr 2003 19:51:59 -0400

> From: "Network Solutions, Inc." [...]

> Subject: Customer Renewal Warning

> Dear Network Solutions(R) Customer,

> We recently learned that our customers are receiving domain name renewal

> notices from companies falsely representing themselves as Network

> Solutions. These notices inform customers that their domain name

> registration is due to expire and provides instructions on how to renew.

> If you receive a renewal notice you do not believe is from Network

> Solutions or if you have an unauthorized vendor listed on your credit card

> statement for 'domain name renewal,' please contact us immediately [...].

✶ Spammers use viruses to hijack computers

"NewsScan" <newsscan@newsscan.com>

Wed, 30 Apr 2003 08:46:57 -0700

As efforts to tackle junk e-mail ramp up, unscrupulous spammers increasingly are hiding their identities by taking over innocent users' accounts using e-mail messages that resemble computer viruses. Like many other viruses, these programs exploit weaknesses in Microsoft's popular Outlook e-mail package. One of the first hijacking programs to emerge was called "Jeem," which contained a hidden e-mail engine that enabled it to route messages via the infected computer. Another, called Proxy-Guzu, comes as a spam message with an attachment. When the unsuspecting recipient clicks on the attachment, the computer contacts a Hotmail account and transmits information about the infected machine, making it possible to route e-mail through that machine. "Spammers are beginning to use virus-like techniques to cover themselves," says Larry Bridwell, content security programs manager at ICSA Labs. "Spam is one of the two things that the security industry is going to be asked to deal with. The other is adware or spyware." [BBC News

30 Apr 2003; NewsScan Daily, 30 Apr 2003]

<http://news.bbc.co.uk/2/hi/technology/2988209.stm>

✶ Breastfeeding mothers, avoid Continental (via Dave Farber's IP)

Meng Weng Wong <mengwong@dumbo.pobox.com>

Tue, 22 Apr 2003 10:50:54 -0400

Deborah Wolfe, a Canadian citizen who was just breast-feeding her son and changing his diaper while en route between Houston and Vancouver, says her "subversive" actions led to her being threatened with detainment, RCMP involvement and legal charges for terrorist action against a U. S. citizen in international airspace while on an American flight during a time of war.

... Wolfe says she refused a flight attendant's offer of an airline blanket to hide herself because it hadn't been sealed and, given the SARS scare, she'd rather use her own things. Thus, unbeknownst to her, a "Level 1" crew complaint was filed. ... She says the flight attendants also began to call her and her travelling party "foreign nationals in international airspace on an international flight during a time of war." And she was informed both of the complaint and that it could be upgraded to a Level 3, which meant possible mandatory detainment by U.S. authorities for 24 hours, RCMP involvement and criminal charges for an act of war upon an American.

<http://www.canada.com/montreal/montrealgazette/story.asp?id=51AA6AB6-034B-4FE0-911C-04871E6B1EC5>

IP archives at: <http://www.interesting-people.org/archives/interesting-people/>

Re: NCIC database accuracy requirements

John Beattie <JKB@hignfy.demon.co.uk>

Mon, 21 Apr 2003 11:01:55 +0100

As reported in [RISKS-22.65](#), etc., the accuracy requirements for the FBI's National Crime Information Center have been reduced or eliminated. Also

discussed in the April 2003 Cryptogram:

<http://www.counterpane.com/crypto-gram-0304.html>

At first sight this is bad. But the other point of view may be worth noting:

a widely used database which is "accurate" but has a high false positive

rate may provide a useful widespread learning experience. Most users of

databases regard "the computer" as infallible. A 100-to-1 false positive

rate would be salutary! :-)

It isn't enough that engineers and computer scientists understand accuracy

requirements; the end-users, as represented by lawyers, have to have a

feeling for it as well. Bad databases already do damage -- it may be that

what is needed is a really high-profile failure.

You can argue probabilities as much as you like; the thing will only hit

home when almost everyone who's had contact with the database has actual

knowledge of a failure.

[Perhaps if a few Senators, Representatives, Justice Department folks,

and other government officials were mistakenly apprehended, that might

help. PGN]

✦ **Re: Friendly Fire (Ladkin, [RISKS-22.68](#))**

"Jan C. =?iso-8859-1?Q?Vorbr=FCggen?=" <jvorbrueggen@mediasec.de>
Mon, 28 Apr 2003 15:58:19 +0200

I believe a technical contribution to this organizational problem was the fact that Aegis computed/computes the first and second derivatives of measured target height to derive sink/climb rate and acceleration. These values, derived as they are from noisy measurements, are notoriously unreliable. The crew seems to have treated these "measurements" at face value, deriving a threat from the fact that they indicated a high sink rate directed at the Vincennes, when in reality the aircraft was flying level. So in this case the misinterpretation (at least in part) resulted in the inability of computers to provide processed but unreliable data, very likely without an indication of its unreliability (ever seen error bars on such displays?).

Jan Vorbrüggen - MediaSec Technologies, Berliner Platz 6-8, D-45127 Essen
Research & Development - Tel. +49 201 437 52 52 <http://www.mediasec.com>

✦ **REVIEW: "Firewalls and Internet Security", Cheswick/Bellovin/Rubin**

Rob Slade <rslade@sprint.ca>

Fri, 25 Apr 2003 08:36:55 -0800

BKFRINSC.RVW 20030321

"Firewalls and Internet Security", William R. Cheswick/Steven M. Bellovin/Aviel D. Rubin, 2003, 0-201-63466-X, U\$49.99/C\$77.99

%A William R. Cheswick ches@cheswick.com

%A Steven M. Bellovin smb@stevebellovin.com

%A Aviel D. Rubin avi@rubin.net

%C P.O. Box 520, 26 Prince Andrew Place, Don Mills, Ontario
M3C 2T8

%D 2003

%G 0-201-63466-X

%I Addison-Wesley Publishing Company

%O U\$49.99/C\$77.99 416-447-5101 fax: 416-443-0948

%O [http://www.amazon.com/exec/obidos/ASIN/020163466X/
robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/020163466X/robsladesinterne)

[http://www.amazon.co.uk/exec/obidos/ASIN/020163466X/
robsladesinte-21](http://www.amazon.co.uk/exec/obidos/ASIN/020163466X/robsladesinte-21)

%O [http://www.amazon.ca/exec/obidos/ASIN/020163466X/
robsladesin03-20](http://www.amazon.ca/exec/obidos/ASIN/020163466X/robsladesin03-20)

%P 433 p.

%T "Firewalls and Internet Security: Repelling the Wily Hacker,
Second Edition"

As the first work to deal seriously and completely with the topic, the first edition of "Firewalls and Internet Security" was one of those classics that get known only by the last names of the authors, so as not to leave any possibility of confusion with books whose titles may be similar.

When such a long time has elapsed between editions of a work such as this, it is more than possible that the field has moved on far enough that a minor updating of the material is simply not feasible. The authors are quite well aware of the new territory: where useful, the original structure has been

retained, but otherwise, the book has essentially been rewritten. A huge undertaking, but the only practical course, in the circumstances.

Part one establishes a starting point. Chapter one, an introduction, presents a number of basic, but worthwhile, security concepts. The operations of various components of the TCP/IP protocol suite are discussed, with the most serious security vulnerabilities helpfully highlighted, in chapters two (lower layers) and three (upper layers). The authors' thoughts on the security of the Web are amply expressed in the title of chapter four: "The Web: Threat or Menace?"

Part two outlines the threats to networked machines. Chapter five describes a number of different types of attacks. A variety of tools for determining security weaknesses are listed in chapter six, alongside discussions of the relative costs/benefits of disclosure versus security by obscurity.

Part three details security tools and utilities. Chapter seven reviews authentication concepts and techniques. Various network security systems are described in chapter eight.

Part four gets us to firewalls and virtual private networks (VPNs) themselves. Chapter nine outlines the different types of firewalls. Basic filtering concepts are examined in chapter ten. Considerations for constructing and tuning your firewall are in chapter eleven. Tunnelling and VPNs are discussed in chapter twelve.

Part five extends the isolated technology of firewalls into the application of protecting an organization. Network layout, and the implications thereof, is reviewed in chapter thirteen. Chapter fourteen deals with hardening of hosts. Chapter fifteen is a rather terse look at intrusion detection.

Part six is entitled "Lessons Learned." The detection and tracing of "berferd" is described in chapter sixteen, along with the taking of the "CLARK" machine in chapter seventeen. In chapter eighteen, Kerberos and IPsec are used as examples of approaches to security of insecure networks. Chapter nineteen finishes with some ideas for work that yet needs to be done to help with the security of the Internet.

The place of firewalls in regard to network security has broadened considerably in the past decade. This book does reflect that reality. Unfortunately, that breadth of topic has come at the expense of some depth in coverage. The result is a book that is definitely worthwhile as an introduction to the field, but which may no longer be suitable as a working reference. I must admit that, for some time, I have been recommending Chapman and Zwicky (cf. BKBUINFI.RVW) over Cheswick and Bellovin's original text, since "Building Internet Firewalls" seems to have the edge in terms of practicality. Upon reviewing this new edition of the classic, I would have to stick to that recommendation.

copyright Robert M. Slade, 1994, 2003 BKFRINSC.RVW 20030321

rslade@sprint.ca rslade@vcn.bc.ca slade@victoria.tc.ca
pl@canada.com

★ **REVIEW: "Inside the Security Mind", Kevin Day**

Rob Slade <rslade@sprint.ca>

Fri, 2 May 2003 08:21:11 -0800

BKINSCMI.RVW 20030321

"Inside the Security Mind", Kevin Day, 2003, 0-13-111829-3,
U\$44.99/C\$69.99

%A Kevin Day

%C One Lake St., Upper Saddle River, NJ 07458

%D 2003

%G 0-13-111829-3

%I Prentice Hall

%O U\$44.99/C\$69.99 +1-201-236-7139 fax: +1-201-236-7131

%O [http://www.amazon.com/exec/obidos/ASIN/0131118293/
robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/0131118293/robsladesinterne)

[http://www.amazon.co.uk/exec/obidos/ASIN/0131118293/
robsladesinte-21](http://www.amazon.co.uk/exec/obidos/ASIN/0131118293/robsladesinte-21)

%O [http://www.amazon.ca/exec/obidos/ASIN/0131118293/
robsladesin03-20](http://www.amazon.ca/exec/obidos/ASIN/0131118293/robsladesin03-20)

%P 309 p.

%T "Inside the Security Mind: Making the Tough Decisions"

I am quite sympathetic to the idea that the realization of a security mindset or attitude (I frequently refer to it as professional paranoia) is more important to attaining security than isolated technical skills. I'm sorry to say that this work is not likely to help you find, attain, or assess that protection perspective.

Right from the beginning of the book, readers will find a

flavour of eastern philosophy, and even mysticism, to it. There are four virtues, an eight-fold path, and even repeated injunctions for the reader to keep an "open mind"--a phrase which those who have conversed with devotees of the Buddhist faith will find rather familiar.

Unfortunately, chapter one seems to demonstrate that Day is bringing us only a newage vagueness in his description of the security mind. We are to rid ourselves of negative thoughts, and follow fundamental virtues, which we haven't been given yet. Computer security is only a decade old, we are told in chapter two, and constantly changing, and expensive, and there are few practitioners, and lots of bad guys out there, and we are paralyzed by fear--but we have nothing to fear but fear itself! Chapter three finally lists the four virtues for us: security is ongoing, a group effort, requires a generic approach, and is dependent upon education. I don't disagree with any of these points (other than the philological debate about whether they should be called virtues), and neither would any other security professional. However, they don't really provide us with much in the way of help. Eight security "rules," in chapter four, list principles such as "least privilege," which are also commonly known in security work.

Chapter five is supposed to tell us how to develop a security mind, but actually seems to be an exercise in wishful thinking. If the world were neatly divided into safe and unsafe zones, and if our systems all worked

perfectly and in correspondence with our users' known requirements, and if everyone that we trusted were completely competent in regard to their own defence, security would be much easier. Decision-making is likewise simplistically seen to be supported by the virtues and rules, in chapter six. There is a superficial overview of blackhats and vulnerabilities in chapter seven. Chapter eight has a standard review of risk analysis. Vague ideas on hiring security, and some thoughts on outsourcing, are in chapter nine. The author gives his opinion on some security tools in chapter ten. Chapter eleven is another attempt to prove that the rules can be used. We are given a final adjuration to change our attitudes in chapter twelve.

Basically, this book is yet another attempt to write a general security guide, without first ensuring that the material is structured, sound, complete, or useful.

copyright Robert M. Slade, 2003 BKINSCMI.RVW 20030321
rslade@sprint.ca rslade@vcn.bc.ca slade@victoria.tc.ca
pl@canada.com



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

[ACM](#) Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 72

Saturday 10 May 2003

Contents

- [Software bug sent Soyuz off course](#)
[Tom Van Vleck](#)
- [Microsoft admits Passport was vulnerable](#)
[Monty Solomon](#)
- [E-mail hoax at University of Maryland](#)
[Paul Kafasis](#)
- [Pair held in plot to steal thousands of identities](#)
[Monty Solomon](#)
- ["Jeff Jackboot" -- more spelling-checker follies?](#)
[Daniel P. B. Smith](#)
- [Misquoting Google](#)
[Monty Solomon](#)
- [T-Mobile Hotspot uses SSN for passphrase](#)
[Conrad Heiney](#)
- [Making it harder for prying eyes](#)
[Monty Solomon](#)
- [Re: Friendly Fire](#)
[Matt Jaffe](#)
- [Re: Patriots and Friendly Fire](#)
[Peter B. Ladkin](#)

- [Re: OpenBSD release protects against buffer-overflow attacks](#)
[Jeremy Ardley](#)
 - [Re: Pilots fail exams](#)
[Don Lindsay](#)
[Vince Mulhollon](#)
[Toby Gottfried](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✈ Software bug sent Soyuz off course

Tom Van Vleck <thvv@multicians.org>
Mon, 5 May 2003 19:42:58 -0400

A mysterious software fault in the new guidance computer of the Soyuz TMA-1 spacecraft was the cause of the high-anxiety off-course landing over the weekend, NASA sources tell MSNBC.com. ONCE IDENTIFIED, the error should be easy to fix in the computer of the Soyuz TMA-2, which is now attached to the International Space Station to provide the new two-man crew with a way to return to Earth..." [Source: James Oberg, NBC News Space Analyst, 5 May 2003]

<http://www.msnbc.com/news/909677.asp>

[I like that "should." THVV]

[Also noted by James Paul and Nancy Leveson. PGN]

[The autopilot suddenly reported it had ``forgotten where it was and which way it was headed'' -- whereupon it switched to backup. The result was a twice-as-rapid deceleration and premature landing. PGN]

Microsoft admits Passport was vulnerable

Monty Solomon <monty@roscom.com>

Fri, 9 May 2003 01:42:20 -0400

Muhammed Faisal Rauf Danka, a computer researcher in Pakistan discovered how to breach Microsoft Corp.'s security procedures for its popular Internet Passport service, designed to protect customers visiting some retail Web sites, sending e-mails and in some cases making credit-card purchases.

Microsoft acknowledged the flaw affected all its 200 million Passport accounts but said it fixed the problem early Thursday, after details were published on the Internet. Product Manager Adam Sohn said the company was unaware of hackers actually hijacking anyone's Passport account, but several experts said they successfully tested the procedure overnight.

In theory, Microsoft could face a staggering fine by U.S. regulators of up to \$2.2 trillion. Under a settlement with the Federal Trade Commission last year over lapsed Passport security, Microsoft pledged to take reasonable safeguards to protect personal consumer information during the next two decades or risk fines up to \$11,000 per violation.

The FTC said it was investigating this latest lapse. The agency's assistant director for financial practices, Jessica Rich, said Thursday that each vulnerable account could constitute a separate violation _ raising the

maximum fine that could be assessed against Microsoft to \$2.2 trillion. ...

[Source: Ted Bridis, Associated Press, 8 May 2003]

<http://apnews.excite.com/article/20030508/D7QTDPQ03.html>

<http://finance.lycos.com/home/news/story.asp?story=34127595>

E-mail hoax at University of Maryland

"Paul Kafasis" <paul@pbones.com>

Sun, 4 May 2003 13:28:07 -0400

It appears that a gaping security hole at the University of Maryland led to an unexpected "canceling" of classes for Friday, April 11th. One or more students sent an e-mail to an address on campus which sent out to 3500 students and had no protection on it. From speaking to students at the school, it appears that they were signed up for an e-mail list without their knowledge, a list which accepted submissions from anywhere. Thursday night (4/10), they began receiving confusing e-mails from each other, trying to unsubscribe from the list. Before the OIT department shut it down, a virus and a hoax e-mail canceling classes for the following day due to "budget cuts" had been sent out.

The culprits even went so far as to spoof the format of other letters sent out campus wide, as well as the headers and reply-to address. As their OIT spokeswoman said:

"E-mail is one of the most easily forged or compromised mediums," she said. "Always verify anything that looks suspicious or strange."

Of course, if the students are correct that this was an open list sending mail to 3500 people, they were just asking for trouble.

<http://www.inform.umd.edu/News/Diamondback/archives/2003/04/14/news2.html>

It looks like the culprits were making a Catch-22 reference to Colonel Cathcart, but no one at the school got it. I found that to be the funniest part of the article.

Pair held in plot to steal thousands of identities

Monty Solomon <monty@roscom.com>

Mon, 5 May 2003 01:07:26 -0400

Federal authorities have arrested an Irvington, New Jersey, man and woman who allegedly schemed to steal the identities of as many as 3,700 clients at one of the nation's largest mortgage companies. FBI agents found credit reports, fake licenses, and recently purchased high-tech equipment. Each bore the names of customers at Weichert Financial Services, the Morris Plains-based company that operates as a partner to Weichert Realtors. One of the suspects has worked as an administrative assistant for the company since May 2001. A federal complaint released yesterday said she and her roommate used a high-speed Internet connection from their home to access more than 500 credit reports of Weichert clients between 11 Jan and 7 Feb

2003. [Source: Article by John P. Martin, Feds charge Irvington couple used the Internet to illegally access credit reports from mortgage firm, *Newark Star-Ledger*, 2 May 2003; PGN-ed]
<http://www.nj.com/news/ledger/jersey/index.ssf?/base/news-3/1051857944181440.xml>

⚡ "Jeff Jackboot" -- more spelling-checker follies?

"Daniel P. B. Smith" <dpbsmith@world.std.com>
Sat, 03 May 2003 20:10:18 -0400

Googling for news, I ran across an opinion piece in an Australian publication by someone styling himself "Jeff Jackboot." This didn't sound like a real surname, and I assumed it to be some kind of curious nom de plume.

The dictionary meanings of "jackboot" are "a stout military boot that extends above the knee," "a person who uses bullying tactics, especially to force compliance," and "the spirit sustaining and motivating a militaristic, highly aggressive, or totalitarian regime or system," and I wondered why this columnist would want readers to make such associations.

On reading further, the piece seemed oddly familiar... and Jeff Jackboot was identified as "a columnist with *The Boston Globe*."

I suddenly realized that this was, in fact, *Globe* columnist Jeff Jacoby.

The Age has not answered my e-mail inquiry about the error. I

suspect this
was probably a spelling-checker error, although my copy of
Microsoft Word
does not not make this correction.

[http://www.theage.com.au/handheld/
articles/2003/04/25/1050777406269.htm](http://www.theage.com.au/handheld/articles/2003/04/25/1050777406269.htm)

(or just do a Google search for "Jeff Jackboot")

✶ Misquoting Google

Monty Solomon <monty@roscom.com>

Sun, 4 May 2003 11:45:08 -0400

Posted, May. 1, 2003

Updated, May. 2, 2003

Misquoting Google

By Jonathan Dube

MSNBC Sr Producer

CyberJournalist.net Publisher

Google has become such a part of our culture that writers often
quote how
frequently a name or phrase appears in a Google search as an
indicator of
popularity. Unfortunately, more often than not, the numbers
published are
completely wrong.

Here are a few examples of Google hit counts being cited in
publications
within the past month. Before you read on, do a search for each
of these
yourself and see if you can figure out if they're in the
ballpark or way
off:

A Google search for the phrase "Iraq war" returns 3.2 million hits.

-- *The Raleigh News & Observer*

"The best defense is a good offense." That favorite saying of heavyweight

champion Jack Dempsey gets a half-million hits on Google... --
*The New
York Times*

The phrase "geopolitical climate" is a favorite among market commentators. A Google search found 1,410 mentions of it. It makes me feel

important to use it. -- *The Motley Fool*

A search on the Google search engine under "boycott American products"

found 117,000 page hits. -- UPI

Most people, when doing searches, fail to put their terms in quotes.

Searching for Iraq War will give you more than 3 million pages, because

Google is searching for any pages that have the words Iraq and War in

them, in any order. Searching for "Iraq War" will give you about 635,000,

because Google is only looking for the exact phrase.

Pulitzer-prize winner Bill Dedman, who runs PowerReporting.com and alerted

me to The New York Times' goof listed above, points out another problem with

not using quotes: Google ignores common words in most searches.

<http://www.poynter.org/column.asp?id=32&aid=32072>

[Ah, yes! We have noted this problem here before. PGN]

⚡ T-Mobile Hotspot uses SSN for passphrase

"Conrad Heiney" <conrad@fringehead.org>

Thu, 8 May 2003 16:20:34 -0700

I just signed up for T-Mobile Wireless' "Hot Spot" service, which provides wireless Internet access via Starbucks Coffee, Borders Books, and many other semi-public places in the U.S. As a current T-Mobile telephone subscriber I was given a good deal. I was also given a user name and a passphrase, neither one of which can be changed. The user name is my telephone number and the pass phrase is the last four digits of my social security number.

The obvious RISK of using the phone number and SSN in this manner is pretty awful (identity theft, etc.) but what's also quite funny is that those are the two things you need to identify yourself to T-Mobile for any other purpose, too. Try again, guys.

Conrad Heiney conrad@fringehead.org <http://fringehead.org>

⚡ Making it harder for prying eyes

Monty Solomon <monty@roscom.com>

Mon, 05 May 2003 20:52:33 -0700

A bill in the California state legislature would protect the anonymity of Internet users by requiring Internet service providers to send customers

copies of subpoenas seeking to learn their identities. If passed, California's Internet Communications Protection Act would become the second state law requiring that consumers be alerted when an ISP is issued a subpoena to find out an anonymous Internet user's true identity. Virginia passed a similar statute last year.

The debate over anonymous online speech has heated to a boil in recent years, with companies and individuals increasingly seeking to have ISPs and Web publishers subpoenaed to learn the names of online critics and people suspected of copyright violations. Yahoo alone expects to receive 600 civil subpoenas this year -- a 50 percent jump from 2002.

Such requests seek a variety of personal information about Internet users, including full names, Social Security numbers, home addresses and pseudonyms they've used online.

The California legislation would require ISPs to send copies of civil subpoenas to their customers by registered mail within 14 days of receiving them. If the customer decides to fight the request, he or she would have 30 days to serve both the ISP and the issuing party with written copies of the objection.

ISPs that fail to comply with the act could be sued by their customers.

Source: Article by Julia Scheeres, New California law regarding anonymous customer information, 5 May 2003; wired.com

<http://www.wired.com/news/politics/0,1283,58720,00.html>

✶ Re: Friendly Fire (Vorbrueggen, [Risks-22.71](#))

Matt Jaffe <jaffem@erau.edu>

Wed, 07 May 2003 06:54:25 -0700

Perhaps I can shed some additional light on the points Mr. Vorbrueggen makes. This subject was touched on quite a while ago in [RISKS-08.74](#), but I think more emphasis was placed there on the problems with the modes and codes than on this discussion of altitude. Although related, the issues are different enough to perhaps warrant some additional discussion here.

The first point to clarify here is that at the time of the Vincennes shoot down, Aegis almost certainly did not display vertical rate or vertical acceleration data to its operators. (The original HMI design as of the EDM-3C PDR in the mid 1970's did not provide that data; of that I am certain.) It displayed computed altitude only (not rate). We debated that issue (adding a vertical rate [but not acceleration] indicator to some of the operational displays) quite heatedly during the design phase for the original Aegis human-machine interface. It was no casual oversight that it was omitted. The reason for the omission was essentially as Mr. Vorbrüggen notes: "These values, derived as they [would have to have been] from noisy

measurements, [would have been] notoriously unreliable."

Since the "rawer" (not by any means raw) initial altitude estimates were intrinsically noisy, a timely display of vertical rate would thus be intrinsically unstable ("It's climbing; no, its descending; no, now it's climbing again; no, now it's descending") and a more stable estimate requiring extensive filtering/damping would be too sluggish of response to be tactically useful. ("Oh, Captain, you'll undoubtedly be pleased to know that the missile that hit us 30 seconds ago was dropped from an aircraft that we now know was descending, not level, when it launched.")

With regard to Mr. Vorbrüggen's comment about error bars: In those prehistoric days, neither the main PPI nor the auxiliary data readout CRT had graphics, color coding, or font variation capabilities. (I think we were on the old AN/UYA-4/OJ-194 series at the beginning). Had we decided (as, after extensive debate, we did not) to provide a vertical rate display, we surely then would have considered generalizing from the old Naval Tactical Data System 2-dimensional track quality indicator (that I believe we retained in 2-D form) to provide a quality indicator for vertical domain data; but there would have been little utility in so doing: At the ranges where the difficult tactical decisions got made, the altitude data (and hence even more so any derived vertical rate estimate) would always have been of the same unvaryingly poor quality. Using scarce tactical display real estate to display such essentially constant information

("low quality vertical rate") would not seem good HMI design.

Overall, after many years, I think the conclusions that I stated in

[RISKS-08.74](#) still stand (the interested reader is referred to the RISKS

archives): Although the expression is overused these days, the fog of war is

very real and there will always be intrinsic limitations on our ability to

design systems (including their organizational and procedural aspects) to

aid in penetrating it. To put such systems into play in ambiguous

environments is to risk catastrophe. But *that* of course, is a political

decision, not a technical, organizational, or operational one.

<http://backoff.pr.erau.edu/jaffem>

⚡ Re: Patriots and Friendly Fire

"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>

Tue, 06 May 2003 13:03:56 +0200

Friendly Fire incidents during armed hostilities have been discussed

in [Risks-22.65](#) (Paul, PGN), [-22.66](#) (Tyson), [-22.67](#) (Eachus, Russ, Youngman), [-22.68](#) (Ladkin, van Meter, Guaspari), [-22.69](#) (Ladkin, Goodall),

much of it concerning the statistics and the interpretation thereof.

There were in total three friendly fire incidents in the 2003 Iraq War

that we know about in which Patriot surface-to-air (SAM) missile systems

are implicated. A UK Royal Air Force Tornado GR4 was shot down by a Patriot on 23 March [1]. On 24 March, a Patriot radar "locked on" to a USAF F-16CJ.

The F-16 destroyed the Patriot battery with an anti-radiation (HARM) missile [1]. In a third incident, in which a US Navy F/A-18C was shot down by a SAM, US Central Command confirmed that a Patriot is suspected [2].

The US Department of Defence's technology chief say that there is a requirement to look at new technology to help prevent friendly fire incidents [3].

Concerning the varying statistics on friendly fire and their interpretation, Col. (ret.) Scott Snook, in his book referenced in my [Risks-22.68](#) note, remarks that 24% (35 out of 148) of all U. S. combat fatalities in the first Gulf War were caused by friendly fire ([4], p11). The 24% figure was repeated by William Safire in his Language column in the International Herald Tribune of 5 May, 2003 [5]. This precision contrasts with the undefined 5% figure of the US Army FM 100-14 which I mentioned in my [Risks-22.69](#) note.

Safire mentions that "In Gulf War II, the rate of [friendly fire] battle deaths dropped to 8 per cent" [5]

There are a number of different phrases used for combat damage caused by one's own side. Safire found a first use of "friendly fire" in an NYT article on April 3, 1944. He mentions that the term "fratricide", seemingly preferred by the military nowadays, "emerged in the press in the

'80s." He notes that there has not yet been a sororicide [5]. It has been called "amicicide" (semantically a more appropriate phrase) by C.R. Shrader in the title of a 1982 book [6]. Flight International has used the phrase "blue on blue" [2,3]. In war games, Safire explains, "friendly" forces are known as "blues", and "enemy" forces as "reds".

References

- [1] Accidents Take Their Toll, Flight International, 1-7 April 2003, p6.
- [2] Flight International, Patriot under fire for second error, 8-14 April 2003, p10.
- [3] Flight International, Science could prevent friendly fire, 15-21 April 2003, p8.
- [4] Scott A. Snook, Friendly Fire: The Accidental Shootdown of U. S. Black Hawks over Northern Iraq, Princeton University Press, 2000. Details at <http://pup.princeton.edu/titles/6847.html>
- [5] William Safire, Of severe/acute: Is the acronym SARS redundant? International Herald Tribune, 05 May 2003, available from [http://www.iht.com/ihtsearch.php?id=95223&owner=\(NYT\)&date=20030505130338|](http://www.iht.com/ihtsearch.php?id=95223&owner=(NYT)&date=20030505130338|)
- [6] C. R. Shrader, Amicicide: The Problem of Friendly Fire in Modern War, Fort Leavenworth, Kansas: U.S. Army Command and General Staff College Press, 1982.

Peter B. Ladkin, University of Bielefeld, Germany

<http://www.rvs.uni-bielefeld.de>

⚡ Re: OpenBSD release protects against buffer-overflow attacks ([R 22-71](#))

"Jeremy Ardley" <jeremy@electrosilk.net>
Sun, 4 May 2003 14:30:51 +0800

It is commendable that the OpenBSD group [*] is doing protecting against buffer overflow attacks.

What is not so apparent is why technology that was developed and operating over 30 years ago is just being re-invented in software.

The Burroughs 6700 implemented a hardware solution to the problem by assigning 3 bits of very 51 bit memory location to the type of data contained.

Memory that was tagged as data could not be executed. The result was that no stack overflow attack was possible.

Today's Intel based fix is appears to be a hack to work around a deficient architecture. The question that arises is why the architecture of today ignores the solid groundwork or previous years?

[Because mass-market operating systems don't use the protection that is available in today's hardware. Note that Multics had a similar execute bit solution in 1965 that prevented execution of data. Executable

attachments are clearly an abomination. PGN]

[* Misattribution now corrected in ARCHIVE COPY. PGN]

✉ **Re: Pilots fail exams ([RISKS-22.71](#))**

Don Lindsay <dlindsay@don-lindsay-archive.org>

Sun, 4 May 2003 00:37:11 +0000 (GMT)

> The pilots couldn't pass the psychological and physical tests
> to be
> allowed to carry a firearm --- but flying huge planes full of
> people is
> OK. Oh, this makes so much sense! The risks should be obvious.

Indeed, it does make sense. It would be risky so assume that one
skill set
implies another.

The two domains (commercial piloting and inflight weapons use)
do have some
things in common. Both require the ability to learn procedure,
and both
require efficient action under stress. But they differ
significantly.
Piloting involves relatively few interpersonal skills, whereas
the use of
weapons requires judgments of motive and threat, discrimination
of
perpetrators from hostages, and the like. Also, piloting can be
done safely
by a bigot, but you don't give police powers to someone who
feels that
everyone in a particular ethnic group is better off dead. Some
people are so
nervous about weapons that their hand shakes, and they can't hit
the broad
side of a barn door. And so on.

I'm pleased that domain-specific testing was applied.

[Also commented on by Bill Hopkins. PGN]

✶ Re: Pilots fail exams ([RISKS-22.71](#))

"Vince Mulhollon" <vlm@norlight.com>

Mon, 5 May 2003 09:03:48 -0500

The belief that carrying a gun and flying an airplane are the same is a false analogy. That makes irrelevant the implication that failures of the gun program are bad pilots.

I can think of several examples which would disqualify a pilot carrying a gun, but not flying a plane.

As for failing the background check, a income tax cheater could be a felon, and felons can't carry. But, an income tax cheat could be an excellent, safe pilot.

As for failing psychological tests, what about a conscientious objector? If a pilot learns during training, that they cannot take a human life, there is no point in giving them a weapon. A pilot whom is unwilling to kill is probably an otherwise safe pilot.

As for physical test failures, the impact load of a pistol is more intense than any other physical task required to fly an airplane. If someone has

experienced stress fractures in their arm or wrist in the past, it would be dumb to give them a .45, as after they shoot the hijacker, they'd likely break their arm again, and then be unable to fly the plane. Or, as an chronic issue, good marksmanship requires regular training, and someone with tendonitis or carpal tunnel should probably not aggravate those problems by regular firearms practice, although the low impact task of flying may be perfectly safe.

Finally as for marksmanship training, the ability to get a bullseye has no relation to piloting ability.

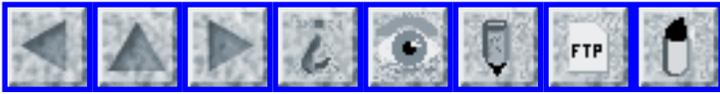
✈ **Re: Pilots fail exams ([RISKS-22.71](#))**

"Toby Gottfried" <toby@gottfriedville.net>

Mon, 5 May 2003 08:27:57 -0700

"Officials said the four rejections showed that the government was serious about providing guns only to pilots who were psychologically and physically fit to carry firearms in flight and defend their planes against attackers."

Can we presume, then, that these four would not be allowed to fly as co-pilots with another pilot who had passed the tests and was armed ?



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

[ACM](#) Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 73

Tuesday 20 May 2003

Contents

- [Time synchronization error leads to mistaken arrests](#)
[Timothy J. Miller](#)
- [U.S. cracks down on Internet fraud](#)
[NewsScan](#)
- [Intel says Itanium 2 error can crash servers](#)
[Monty Solomon](#)
- [MS Windows crash traps Thai politician in car](#)
[Robert J. Berger via Dave Farber](#)
- [Internet worm disguised as e-mail from Microsoft](#)
[Monty Solomon](#)
- [Microsoft toilet project wasn't hoax](#)
[NewsScan](#)
- [The Exterminator](#)
[Monty Solomon](#)
- [Immature air-traffic controllers?](#)
[Carl Fink](#)
- [The Great Capacitor Scare of 2003](#)
[Jay R. Ashworth](#)
- [Los Altos Vault & Safe Deposit Co.](#)
[Drew Dean](#)

- [Risk of automatic type conversion](#)
[Dave Brunberg](#)
 - [Earthlink awarded \\$16M in spamages](#)
[NewsScan](#)
 - [Potential Chilling Effect: IEEE publications and DMCA](#)
[Sean Smith](#)
 - [Re: OpenBSD release protects against buffer-overflow attacks](#)
[Mike Albaugh](#)
 - [Re: more spelling-checker follies?](#)
[Bill Hopkins](#)
[Bill Stewart](#)
 - [REVIEW: "802.11 Security", Bruce Potter/Bob Fleck](#)
[Rob Slade](#)
 - [REVIEW: "Mobile VPN", Alex Shneyderman/Alessio Casati](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Time synchronization error leads to mistaken arrests

"Timothy J. Miller" <cerebus@sackheads.org>

Tue, 20 May 2003 11:11:31 -0500

<http://www.azstarnet.com/star/Tue/30520SIERRAVISTACHARGES.html>

A grainy picture from an ATM surveillance camera aired by TV's "America's

Most Wanted" connected three Sierra Vista residents to a June 2002

strangulation murder of a woman in Maryland. The mom, daughter and

friend, authorities had said, were believed to have been trying to use the

murder victim's bank card. The problem with that link, investigators now

concede, is that the time recorded by the camera was three minutes off the

time recorded by the ATM.

The risks should be obvious; critical logs should be reliably synchronized either to each other or an independent source.

[For non-ATM users, here ATM means Automated Teller Machine, although this bank transaction seems to have created a new form of Asynchronous Transfer Mode. Perhaps another use of the acronym might be Awfully Terrible Monitoring. PGN]

✶ U.S. cracks down on Internet fraud

"NewsScan" <newsscan@newsscan.com>

Fri, 16 May 2003 09:44:28 -0700

The Justice Department has charged more than 130 people with perpetrating a variety of Internet scams, as well as identity theft and failure to deliver goods purchased online. The crackdown, dubbed Operation E-Con, involved more than 90 investigations involving 89,000 victims whose losses totaled at least \$176 million. In one case, the suspects used a Web site to sell more than \$2 million worth of pharmaceutical drugs without any prescriptions or physician involvement with the purchasers. In another scam, about 400 men lost about \$3,000 each when they sent money off in the hope of winning the hand a Russian bride. Other scams promoted fraudulent investment opportunities, Ponzi-type pyramid schemes and the illegal sale of copyright-protected software, games and movies. Officials say they've

managed to recover about \$17 million from alleged perpetrators.

[AP/Siliconvalley.com, 16 May 2003; NewsScan Daily, 16 May 2003]

<http://www.siliconvalley.com/mld/siliconvalley/news/editorial/5876738.htm>

⚡ Intel says Itanium 2 error can crash servers

Monty Solomon <monty@roscom.com>

Tue, 13 May 2003 00:48:12 -0400

Intel Corp. said that a flaw in some of its Itanium 2 microprocessors could cause systems running the high-end chip to shut down or crash under certain conditions. [Source: Matthew Fordahl, AP, 12 May 2003]

<http://finance.lycos.com/home/news/story.asp?story=34164664>

⚡ MS Windows crash traps Thai politician in car (From Dave Farber's IP)

"Robert J. Berger" <rberger@ibd.com>

Tue, 13 May 2003 17:31:11 -0700

Crashed Computer Traps Thai Politician, 14 May 2003

<http://aardvark.co.nz/daily/2003/n051301.shtml>

Thailand's Finance Minister Suchart Jaovisidha had to be rescued today from inside his expensive BMW limousine after the onboard computer crashed, leaving the vehicle immobilized.

Once the computer failed, neither the door locks, power windows nor air conditioning systems would function, leaving the Minister and his driver trapped inside the rapidly heating vehicle.

Despite the pair's best efforts, it took a full ten minutes before they were able to summon the attention of a nearby guard who freed the two men by smashing one of the vehicle's windows with a sledgehammer.

A report (http://www.bangkokpost.com/Business/13May2003_biz12.html) published in the *Bangkok Post* indicates that the vehicle was Mr Jaovisidha's own BMW 520 which was being used while his state-supplied Mercedes, was being repaired.

BMW's more up-market 7-series range uses a computer system called i-drive which has Microsoft's WindowsCE at its core.

<http://www.microsoft.com/presspass/press/2002/Mar02/03-04BMWpr.asp>

Did Mr Jaovisidha narrowly miss being killed by the blue windscreen of death?

Robert J. Berger - Internet Bandwidth Development, LLC.
Voice: 408-882-4755 eFax: +1-408-490-2868
<http://www.ibd.com>

IP Archives at: <http://www.interesting-people.org/archives/interesting-people/>

[At least 33 readers have noted this one thus far. TNX! PGN]

Internet worm disguised as e-mail from Microsoft

Monty Solomon <monty@roscom.com>

Mon, 19 May 2003 23:07:00 -0400

A new computer worm that disguises itself as an e-mail from Microsoft Corp. is spreading, computer security firms warned on Monday. The e-mail containing the worm, dubbed Palyh or Mankx, appears to come from support@microsoft.com, but is not from the software company. When the attachment is opened, the worm copies itself to the Windows folder, scoops up e-mail addresses from the hard disk and starts sending itself out, said U.K.-based Sophos. The malicious program can spread itself to other Windows machines on a local area network. [Source: Reuters, 19 May 2003] <http://finance.lycos.com/home/news/story.asp?story=34253416>

Microsoft toilet project wasn't hoax

"NewsScan" <newsscan@newsscan.com>

Wed, 14 May 2003 09:53:32 -0700

Microsoft and its public relations firm are now saying that what they themselves thought was a hoax (the development of the iLoo, a portable toilet complete with wireless keyboard and Internet access) actually was a real project of the company's MSN group in the UK. The original press release indicated that the iLoo would offer its users "a unique experience." An MSN product manager now says: "We jumped the gun basically yesterday in

confirming that it was a hoax and in fact it was not," said Lisa Gurry, MSN group product manager. "Definitely we're going to be taking a good look at our communication processes internally. It's definitely not how we like to do PR at Microsoft." In any event, whether really a hoax or really real, the project is now dead -- flushed, as it were. [AP/*USA Today*, 14 May 2003; NewsScan Daily, 14 May 2003]

http://www.usatoday.com/tech/news/2003-05-14-illoo-hoax-retract_x.htm

The Exterminator

Monty Solomon <monty@roscom.com>

Thu, 15 May 2003 09:14:04 -0400

Bug-ridden programs are savagely costly. Microsoft engineer Amitabh Srivastava may have just what we need--a software insecticide.

A strange thing happened last spring to the Board of Directors Web page of furniture maker Herman Miller, Inc. Instead of seeing the company's quarterly numbers, staffers saw a Star of David and a sad face. The chief executive thought someone was mocking his Protestant faith. Computer security chief Dennis Peasley thought, "This has to be a hack." But it was no hack, just a software glitch in how Microsoft's PowerPoint program recognized Herman Miller's custom fonts.

Amitabh Srivastava, a computer scientist deep inside Microsoft

Research, is the guy Microsoft is counting on to automate and accelerate the process of purging mistakes. "The impression is that we don't write very good software," says Srivastava. "Every time my computer crashes, it is a reminder of my failure."

Computer bugs have been around since malfunctions in a 1945 [Harvard] Mark II were blamed (facetiously) on a moth trapped in a relay. Nowadays the term refers to programming flaws--commands that don't accomplish the desired result because computers have a habit of following the letter rather than the spirit of the instructions handed to them. The cost to customers of these flaws is necessarily a nebulous figure, but for what it's worth a National Institute of Standards & Technology report puts it at \$38 billion a year. Evaluating only the cost of intrusions by hackers, who exploit flaws in computer security, Gartner Group comes up with \$5.4 billion a year.

Srivastava's fix is an arsenal of tools that help code testers fumigate buggy code. He has a big fan in Microsoft Chairman Bill Gates. "Software quality is about removing or preventing defects. The sooner any defect is caught, the better--ideally, they are simply never coded," says Gates.

Building clean code is getting more daunting, especially for Microsoft . The Windows operating system has 50 million lines of code (a line averages 60 characters) and grows 20% with every release. It's put together by 7,200

people, comes in 34 languages and has to support 190,000 devices--different models of digital cameras, printers, handhelds and so on. ...

[Source: Lycos.com, 26 May 2003]

<http://finance.lycos.com/home/news/story.asp?story=34131541>

✶ Immature air-traffic controllers?

Carl Fink <carl@fink.to>

Tue, 20 May 2003 13:36:05 -0400

Reuters reports that pilots approaching Luton airport were hearing a baby's cries instead of instructions from the controllers.

It turned out that a baby monitor, in a house in the approach path, was being picked up by their radios. Replacing the monitor fixed the problem, so seemingly it was transmitting on the wrong frequency.

The article says that no one was endangered because the pilots could switch to another frequency. My question: exactly how powerful a transmitter is in this baby monitor if a plane moving at hundreds of kilometers per hour would stay in its "radius of interference" long enough to have to switch frequencies?

<http://news.excite.com/odd/article/id/327280|oddlyenough|05-20-2003%3A%3A10%3A44|reuters.html>

Carl Fink <http://www.jabootu.com> carl@fink.to

✶ The Great Capacitor Scare of 2003

"Jay R. Ashworth" <jra@baylink.com>

Tue, 20 May 2003 16:44:19 -0400

In [RISKS-19.13](#), Mich Kabay quoted the *EE Times* on "The Great Capacitor

Scare Of 1997". People were building motherboards without enough power

supply filter caps, it seems, and machines were locking up.

Oh, to have problems that minor again...

The Great Capacitor Scare of 2003 is going to be *much* worse.

It seems, according to several news stories (linked at the end) that a

materials chemist who worked for a Japanese company, Rubycon Corporation --

which manufactured electrolyte for electrolytic (! :-)
capacitors -- left

his employ, and ended up working for a Chinese capacitor maker, Luminous

Town Electric. (These names tend to sound quaintly amusing to USAdian ears,

which might not be accidental...)

Apparently, in a fairly clear case of corporate espionage, the fellow's

cow-orkers then "defected with the formula" (PCN says, in a confusing bit;

defected to where he was?), and began to sell the electrolyte to many

Taiwanese capacitor makers.

Alas, there was one small problem.

The formula wasn't *complete*. The capacitors, which ought to have been

good (in some cases) for up to 4000 hours, were failing in half that -- or,

if you believe Intel, in as little as 250 hours.

The electrolyte apparently outgasses hydrogen, and pops the seals on the cap, leaking electrolyte onto the board. The missing ingredient was the one which prevented this. I'd speculate that this might not be a point-catastrophic failure... these caps might pop and leak out slowly, shorting out circuits.

But it's even worse.

The Inquirer may put it best:

It is not currently known how many market segments may have been affected by these poor parts, which can be found in motherboards, switchmode power supplies, modems and other PC boards.

The failures of the aluminum capacitors might just be the 'tip of the iceberg,' says Zogbi. "Other component failures from low-cost Asian suppliers might be forthcoming," he warns.

Around 30 per cent of the world's supply of aluminum capacitors is manufactured in Taiwan, according to the Paumanok Group. Confusion over which manufacturers may have used the faulty electrolyte is sending buyers back to Japan to source their capacitors.

The extent of the problem in product that has already shipped won't become clear until components start failing, which may not happen until halfway through the products' life expectancy.

But even *that* may understate the problem...

How many electronic products do *you* know of that use electrolytic capacitors? The RISKS are so obvious that I don't even have to say "The RISKS are obvious". [But you did anyway! PGN]

The Inquirer coverage is at <http://www.theinquirer.net/?article=6085>

Passive Component News is at <http://www.niccomp.com/taiwanlowesr.htm>

Check out the tenor of the editorial footnote; it's as classic as it is uncommon.

TTI, who bill themselves as "The world's leading distributor of Passive, Interconnect, and Electromechanical components" have put up an entire page tracking press coverage of the issue:

http://www.ttiinc.com/MarketEye/Aluminum_Cap_Issue.asp

Jay R. Ashworth, The Suncoast Freenet, Tampa Bay, Florida
<http://baylink.pitas.com> jra@baylink.com +1 727 647 1274

Los Altos Vault & Safe Deposit Co.

Drew Dean <ddean@csl.sri.com>
Sun, 18 May 2003 13:11:49 -0700 (PDT)

The Los Altos Vault & Safe Deposit Company has been running an ad in local newspapers (here from the May 14, 2003, Los Altos Town Crier, p. 12) with the following:

"It is impossible for hackers to penetrate our computer system.
Reason -

We have no computers. We do business the old fashioned way."

Now that's a convincing assurance argument! I find it quite interesting that this is being advertised to the general public, or at least that portion living in Silicon Valley.

On the other hand, the old fashioned way has its own risks, but those aren't mentioned. Again, interesting from a marketing viewpoint.

Drew Dean, Computer Science Laboratory, SRI International

⚡ Risk of automatic type conversion

Dave Brunberg <DBrunberg@FBLEOPOLD.com>

Fri, 16 May 2003 11:20:32 -0400

I recently downloaded a copy of an MSDS document for a particular chemical used frequently in water treatment. While scanning through the pages I noticed the following:

"US Patent No. 5E + 06"

I can only assume (bad policy?) that this is related to the document being automatically generated from a database of chemical information.

A quick look at the rest of the document showed no obvious errors, but in something as potentially important to health and safety as an MSDS, one would expect better proofreading by the distributor. That's not to mention any legal problems they may run into regarding disclosure of product

hazards.

David W. Brunberg, Engineering Supervisor - Field Process
The F.B. Leopold Company, Inc.

✶ Earthlink awarded \$16M in spamages

"NewsScan" <newsscan@newsscan.com>

Thu, 08 May 2003 09:23:09 -0700

A federal judge awarded Earthlink \$16.4 million in damages and instituted a permanent injunction against a Buffalo, NY, man identified as the ringleader of a group that used Earthlink's network to send 825 million spam messages over the past year. Earthlink said Howard Carmack and his cronies used Internet accounts opened with stolen identities and credit cards to send junk e-mail. The ruling is the latest in a series of legal actions taken by ISPs against bulk spammers. Last year Earthlink won \$25 million in damages in a suit against another bulk e-mailer, Kahn C. Smith of Tennessee, but it hasn't collected the award. The company also has several other lawsuits pending. Meanwhile, last December, America Online won a \$6.9 million judgment against a now-defunct Illinois company that specialized in p*rnographic spam. Over the last few years, AOL has won 25 spam-related lawsuits against more than 100 companies and individuals, says a company spokesman. [AP 7 May 2003; NewsScan Daily, 8 May 2003]

<http://apnews.excite.com/article/20030507/D7QSJOQ80.html>

✂ Potential Chilling Effect: IEEE publications and DMCA

Sean Smith <sws@cs.dartmouth.edu>

Fri, 16 May 2003 12:48:18 -0400

This morning, I noticed that in the IEEE copyright form (which authors must sign when they publish papers with the IEEE), the signer must warrant that "publication or dissemination of the work" will not violate the DMCA.

Sean W. Smith, Ph.D. sws@cs.dartmouth.edu <http://www.cs.dartmouth.edu/~sws/>

Department of Computer Science, Dartmouth College, Hanover NH USA

✂ Re: OpenBSD release protects against buffer-overflow attacks

Mike Albaugh <albaugh@spies.com>

Mon, 12 May 2003 13:47:48 -0700 (PDT)

> [Ardley: over 30 years ago ... reinvented in software...]

WELL OVER 30 years ago, considering that the machine described in the "First Draft" paper on EDVAC (leaked by John von Neumann) was "tagged", in a sense.

Every word of memory was meant to be designated as "Instruction" or "Data"

during the program-loading process. It was not exactly the way we think of

such things today. An attempt to "execute data" produced not an exception

but effectively a "load immediate", while an attempt to "store to an

instruction" altered only the address-part of the word. Yes, chilluns, this was before B-Boxes :-)

> Memory that was tagged as data could not be executed. The result
> was that no stack overflow attack was possible.

This ignores the prevalence of interpreted "data", the basis of numerous email and web malware. There is still plenty of mischief that can be done without the ability to "execute the stack", and some utility in being able to convert from data to executable, vis. work by David Keppel, et al.

(<http://citeseer.nj.nec.com/78783.html>)

"They may make it illegal, but they'll never make it unpopular" (as noted in another context, in [RISKS-10.27](#)).

[The Harvard Mark I went even further. There were programs in program store and there were data words in data store. And ne'er the twain could meet. PGN]

⚡ Re: more spelling-checker follies? (Smith, [RISKS-22.72](#))

"Bill Hopkins" <whopkins@wmi.com>
Tue, 20 May 2003 17:09:42 -0400

For three minutes, an AP story posted on *The New York Times* Web site about Justice Clarence Thomas referred to his predecessor as "Turgid Marshall."
After checking that MS Word indeed deemed "Thurgood" a

misspelling and suggested "turgid" as a replacement, I discovered that the story had been updated to use the correct name of the distinguished jurist.

✶ Re: more spelling-checker follies? (Smith, [RISKS-22.72](#))

Bill Stewart <bill.stewart@pobox.com>

Sat, 10 May 2003 19:44:06 -0700

A long long time ago, on a Microsoft Mail version far far obsolete by now, I forwarded a copy of my department's org chart to somebody. Unfortunately, MS.Mail decided to spell-check the message and change anything it didn't like without checking with me first. So, it not only changed any of the names it didn't recognize to words it did, including my department head's name, it also changed her Org Chart to an Orgy Chart.

Fortunately, either nobody read it carefully, or they ignored it, so there weren't embarrassing explanations to be made, but my attitude did change from "Lousy unreliable mail client" to "Bill Gates Must" [Verb deleted by moderator for RISKS-obvious reasons. PGN] MS.Outlook is much better than its earlier versions, though it's still fundamentally flawed in a few areas.

✶ REVIEW: "802.11 Security", Bruce Potter/Bob Fleck

Rob Slade <rslade@sprint.ca>

Tue, 13 May 2003 08:03:48 -0800

BK8021SC.RVW 20030404

"802.11 Security", Bruce Potter/Bob Fleck, 2003, 0-596-00290-4,
U\$34.95/C\$54.95

%A Bruce Potter

%A Bob Fleck

%C 103 Morris Street, Suite A, Sebastopol, CA 95472

%D 2003

%G 0-596-00290-4

%I O'Reilly & Associates, Inc.

%O U\$34.95/C\$54.95 800-998-9938 fax: 707-829-0104 info@ora.com

%O <http://www.amazon.com/exec/obidos/ASIN/0596002904/>

[robsladesinterne](#)

<http://www.amazon.co.uk/exec/obidos/ASIN/0596002904/>

[robsladesinte-21](#)

%O <http://www.amazon.ca/exec/obidos/ASIN/0596002904/>

[robsladesin03-20](#)

%P 176 p.

%T "802.11 Security"

The preface states that this book is aimed at the network engineer,

and the security engineer, or the hobbyist, but it is not an introductory work. The reader will need to know Linux to the kernel

configuration level, and TCP/IP networking to the ARP (Address Resolution Protocol) level.

Part one addresses the basics of 802.11 security. Chapter one provides a background, and looks at issues, in wireless communications, although primarily from a communications, rather than

security, perspective. There is a review of attacks and risks, in

chapter two, and for once there is a comparison of wired versus wireless hazards, ranging from the common (interference from portable

phones) to the sophisticated (signal strength attacks related to

diversity antennae).

Part two deals with station, or remote device, security. Chapter three examines attacks against machines and networks, and suggests the use of SSL (Secure Sockets Layer) and SSH (Secure SHell). Configuration recommendations for the kernel, startup, firewall, and other aspects of FreeBSD are covered in chapter four. Chapters five, six, and seven do the same for Linux, OpenBSD, and Mac OS X, respectively (with a concentration on the AirPort utilities for the Mac). Windows, in chapter eight, reviews basic workstation items only, with limited advice and direction.

Part three looks at access port security, and the setup of access points under Linux, FreeBSD, and OpenBSD are all contained in chapter nine.

Gateway security is the topic of part four, with chapter ten looking at gateways and firewalls, while the use of the three UNIX variants as gateways is discussed in chapters eleven, twelve, and thirteen. Authentication and encryption, mostly with IPsec, is reviewed in chapter fourteen. A rather vague closing is given in fifteen.

As noted, this is not a book for beginners. Presumably readers should already know the most common dangers of wireless LANs, such as allowing default access passwords to remain active, and broadcasting the station set identifier. WEP (Wired Equivalent Privacy) is dismissed as irrelevant: since it is deeply flawed, one can assume that the concentration on technologies such as IPsec and station security is of greater use than suggesting minor improvements in the use of WEP keys and initialization vectors. However, it is a bit of a pity that the authors took this route. With the addition of

possibly
an extra fifty pages this could have been an excellent reference
for
all wireless LAN administrators.

copyright Robert M. Slade, 2003 BK8021SC.RVW 20030404
rslade@sprint.ca rslade@vcn.bc.ca slade@victoria.tc.ca
pl@canada.com

★REVIEW: "Mobile VPN", Alex Shneyderman/Alessio Casati

Rob Slade <rslade@sprint.ca>
Thu, 15 May 2003 07:59:40 -0800

BKMBLVPN.RVW 20030401

"Mobile VPN", Alex Shneyderman/Alessio Casati, 2003, 0-471-21901-0,

U\$45.00/C\$69.95/UK#33.50

%A Alex Shneyderman

%A Alessio Casati

%C 5353 Dundas Street West, 4th Floor, Etobicoke, ON M9B 6H8

%D 2003

%G 0-471-21901-0

%I John Wiley & Sons, Inc.

%O U\$45.00/C\$69.95/UK#33.50 416-236-4433 fax: 416-236-4448

%O <http://www.amazon.com/exec/obidos/ASIN/0471219010/>

[robsladesinterne](#)

<http://www.amazon.co.uk/exec/obidos/ASIN/0471219010/>

[robsladesinte-21](#)

%O <http://www.amazon.ca/exec/obidos/ASIN/0471219010/>

[robsladesin03-20](#)

%P 330 p.

%T "Mobile VPN"

Part one presents wireless data fundamentals. Chapter one gives an
introduction to mobile virtual private networks (MVPN), and the

emphasis on cellular technology points out that the authors are familiar with the telecommunications, rather than security, field of work. The material contains a weak suggestion that MVPNs may be useful, lots of alphabet soup, and very little in the way of conceptual background. The data networking technologies in chapter two are not explained very clearly: basic ideas get bogged down with details. Cellular radio interfaces are listed in chapter three, with data services that can be provided over cellular networks in chapter four.

Part two looks at MVPN and advanced wireless data services. MVPN fundamentals, in chapter five, basically reiterates the text from chapter two, with a little extra emphasis on virtual private networks. Chapter six describes various GSM (Global System for Mobile communications)/GPRS (General Packet Radio Service) and UMTS (Universal Mobile Telecommunication System) offerings. Options for CDMA2000 (Code Division Multiple Access) are listed in chapter seven. Chapter eight explains MVPN equipment components and requirements. Possible developments in mobile VPN are advanced in chapter nine.

This book once again emphasizes the divide not only between the cellular and wireless LAN camps, but also between communications and security. It fails to bring all the related technologies together between two covers. At the same time, for those in the LAN or security fields who need to know about cellular service offerings, this work does not provide a

consistent level of explanation and depth of background for those issues. Possible utilities are tabulated, but these could be obtained from almost any cell company sales office.

copyright Robert M. Slade, 2003 BKMBLVPN.RVW 20030401
rslade@sprint.ca rslade@vcn.bc.ca slade@victoria.tc.ca
pl@canada.com



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 74

Wednesday 28 May 2003

Contents

- [Soyuz landing problem caused by software?](#)
[Steve Bellovin](#)
- [The "no-fly" list](#)
[Steve Bellovin](#)
- [Scientific American article "Self-Repairing Computers"](#)
[Charles Lamb](#)
- [Microsoft Pulls XP Update](#)
[Dave Aronson](#)
- [Modern Computers, Unsafe at any speed?](#)
[Len Spyker](#)
- [Privacy advocates doubt Pentagon promises on spying](#)
[NewsScan](#)
- ['Kingpin' cracker arrested in Thailand](#)
[NewsScan](#)
- [Ex-student fined more than \\$500,000 for stock fraud on Net](#)
[NewsScan](#)
- [Safe-cracking via telephone](#)
[Lee Hasiuk](#)
- [Re: OpenBSD ... protects against buffer-overflow ...](#)
[Crispin Cowan](#)

[Dag-Erling Smorgrav](#)

- [Comment on BMW/MSFT failure reported in Risks 22.73](#)

[John Opie](#)

- [Spam's cure could be worse than the disease](#)

[NewsScan](#)

- [Spam limiting](#)

[Harry Hochheiser](#)

- [Re: more spelling-checker follies?](#)

[Anna Shefl](#)

- [REVIEW: "Protected Internet, Intranet, and Virtual Private Networks", Alexander Moldovyan et al.](#)

[Rob Slade](#)

- [Survivable and Self-Regenerative Systems: workshop](#)

[Doug Maughan](#)

- [Info on RISKS \(comp.risks\)](#)

✶ Soyuz landing problem caused by software?

Steve Bellovin <smb@research.att.com>

Mon, 05 May 2003 21:41:08 -0400

In an article by James Oberg -- a well-respected space programanalyst -- MSNBC reports that the cause of the Soyuz module landing far off target was a software glitch. (<http://www.msnbc.com/news/909677.asp?cp1=1>)

To achieve the proper landing profile, the craft is supposed to fly with the top of its heat shield tilted forward, to provide a bit of aerodynamic lift. Steering is done by rotating the capsule -- the center of mass is off-center, whcih means that rotating the Soyuz will steer it.

This scheme means that the Soyuz needs to know which way is up. The Soyuz lost track of either its orientation or its position, and

switched to a backup mode. In the backup setting, the craft just rotates at a constant speed, which stabilizes the spacecraft, but at the cost of path control.

Other suggestions are human error -- perhaps "one of the Americans" hit the backup mode button. The American astronauts deny this.

They did know what was going on; however, they had enough confidence in the backup system that they chose to accept the off-target landing rather than try to recover manually.

Steve Bellovin, <http://www.research.att.com/~smb> (me)

✈ The "no-fly" list

Steve Bellovin <smb@research.att.com>

Fri, 25 Apr 2003 23:03:58 -0400

The 22 Apr 2003 *Wall Street Journal* had a long article on the U.S.

"no-fly" list -- a list of about 300 people that the U.S. government regards

as too dangerous to allow on airplanes. Apart from anything else, the

article discussed the many ways this system is producing false positives and

(one would assume) the chance of false negatives.

The article is too long to summarize; among the problems cited are the

difficulties of transliteration from Arabic (they show five different

renderings of one name) and use of computer systems designed for

different purposes. For example, some of the systems used hunts for matches based on the first few letters of a surname -- ideal for helping someone check in quickly, but not good for checking against a "no fly" list. Nor are the error recovery processes good; there are some people who will *always* run afoul of this on certain airlines, but they seem incapable of recording that they've checked out particular individuals the previous time.

Steve Bellovin, <http://www.research.att.com/~smb>

✶ Scientific American article "Self-Repairing Computers"

Charles Lamb <clamb@acm.org>
Thu, 22 May 2003 17:02:40 -0400

There is an article in the June 2003 issue of "Scientific American" titled "Self-Repairing Computers" by Armando Fox and David Patterson. The article seems to me to just be rehash of decades old programming practices such as audit trails, system snapshots, and robust software. These practices were often found in mainframe computer software but seem to have been abandoned when PCs came along. I suspect this is because mainframe computer time was so much more expensive than PC time that it was worth using more wisely.

✶ Microsoft pulls XP update

Dave Aronson <dja2003@hotpop.com>

Wed, 28 May 2003 14:06:19 -0400

Microsoft Corp. said on 27 May 2003 that it has withdrawn a security update for its Windows XP software after discovering that it switched off Internet connections for some of the 600,000 users who downloaded and installed it.

Source: Reuters. More details at

http://news1.iwon.com/tech/article/id/201872__|technology|05-28-2003%3A%3A00%3A12|reuters.html

Yet another RISK of being an "early adopter" -- especially where a company has a "wait for release x.1" reputation....

David J. Aronson, Unemployed Software Engineer near Washington DC
<http://destined.to/program/>

✶ Modern Computers, Unsafe at any speed?

"Len Spyker" <redmond2@iinet.net.au>

Sun, 25 May 2003 10:25:02 +0800

Periodically we see new emphasis placed on the notion that computers need specific hardware support in order to be secure. So it's odd that when a topic like stack buffer overflows gains common awareness we (the computer community) can always point to a long ago hardware architecture that solved this problem.

It is not like we don't know how to make computers safe. Maybe some of us have buckled to commercial greed, or be unwilling to accept that hardware architecture of 30-50 years ago is still valid today.

I do marvel at my new 1 GHz CPU with it's 30+ million transistors, but I gringe that not a single one is dedicated to preventing the stack from running riot over my own data and code. Or if it had any then the OS writers left it disabled. "Look Ma - no hands".

I feel that the computer industry and PC users are now at the same point that the American Automotive industry was with Ralph Nader some 30-40 years ago. "Unsafe at any speed". But sadly there is no champion now, no one dares to expose that the PC Emperor has no clothes.

The irony is that with proper hardware protection the OS and apps would run faster because all that software now wasting CPU time checking for overflows is no longer needed, and even the most baroque but popular languages could safely co-exist with secure applications.

The only possible good effect from this war on terror is that the OS writers and their bosses may be forced to fully use the hardware protection available and the Silicon designers forced to read some history books and re-invent the hardware wheel.

To correct the current unsecure PC situation will take a major government action and wether it is done by force of law, at legal gun point or by

chucking lots of money at the suppliers to correct their earlier sins and omissions, only time will tell.

Len Spyker, 49 Jeanes Rd, Karrinyup, WA Australia +61 8 9245 1771

✶ Privacy advocates doubt Pentagon promises on spying

"NewsScan" <newsscan@newsscan.com>

Wed, 21 May 2003 09:20:33 -0700

The Pentagon has changed the name of its planned anti-terrorist surveillance systems, but critics say the fundamental program remains the same and would risk violating citizens' privacy if fully implemented. Now renamed the Terrorist Information Awareness program (from Total Information Awareness), the system would broaden government surveillance activities to encompass passport applications, visas, work permits, driver's licenses, car rentals and airline ticket purchases as well as databases including vast amounts of personal information, such as financial, education, medical and housing and identification records. Sen. Ron Wyden (D-Ore.), a major opponent of the TIA, says, "What most Americans don't know is that the laws that protect consumer privacy don't apply when the data gets into government's hands. Lawfully collected information can include anything, medical records, travel, credit card and financial data." Testing of the system is already underway, raising privacy advocates' concerns about "false positives" based

on erroneous data. "If TIA is relying on personal information contained in databases to determine whether someone is a suspect, what recourse does that person have whose information has been entered incorrectly?" says a spokeswoman for the Free Congress Foundation, which estimates that an error rate as small as .10% could result in more than 30,000 Americans wrongly being investigated as terrorists. [AP 20 May 2003;NewsScan Daily, 21 May 2003]

<http://apnews.excite.com/article/20030520/D7R5BBUG0.html>

✶'Kingpin' cracker arrested in Thailand

"NewsScan" <newsscan@newsscan.com>

Fri, 23 May 2003 08:29:25 -0700

Thai officials arrested a Ukrainian man described by a U.S. embassy spokesman as a "kingpin" of international computer crime. Maksym Vysochansky, 25, is accused of selling counterfeit versions of flagship software products by major companies such as Microsoft and Adobe. Vysochansky, who used a number of aliases, is thought to have been involved in fraudulent schemes worth up to \$1 billion. "This guy was on the U.S. Secret Service's 10 most wanted list. He's definitely a big shot," said the embassy official. Authorities allege that Vysochansky also built a "back door" into the software he sold that allowed him to hack into buyers' financial and credit card information. "It was a very complicated and sophisticated fraudulent scheme," said the embassy official.

Vysochansky

likely will be extradited to the U.S. where he'll face charges of copyright violations, trafficking in counterfeit goods and money-laundering.

[News24.com 22 May 2003; NewsScan Daily, 23 May 2003]

http://www.news24.com/News24/Technology/News/0,,2-13-1443_1362931,00.html

✶ Ex-student fined more than \$500,000 for stock fraud on Net

"NewsScan" <newsscan@newsscan.com>

Thu, 22 May 2003 08:02:27 -0700

Former UCLA student Refael Shaoulian has been ordered by a federal judge to pay \$534,000 in fines for using university computers and false identities to post intentionally incorrect about stocks so that he could profit from the buying and selling sprees he caused. The civil suit was brought by the Securities and Exchange Commission. [APOnline/*USA Today*, 22 May 2003;

NewsScan Daily, 22 May 2003]

http://www.usatoday.com/tech/techinvestor/2003-05-21-bruin-amuck_x.htm

✶ Safe-cracking via telephone

Lee Hasiuk <lhasiuk@alumni.caltech.edu>

Thu, 22 May 2003 10:46:50 -0400

My elderly aunt owns a large, heavy safe whose combination was lost when her husband passed away. She asked me if I could help her open it. I called the manufacturer and found that they offer a service where they will give you the combination for \$35, which may be charged to any major credit card. All you need to provide is the safe's serial number, which is embossed on a plate in the center of the combination dial. They have no way of checking if you are the owner of the safe, and indeed I wasn't. The entire transaction took place over the phone. I've yet to try the combination they read to me, and the company representative noted that it is possible for the owner to change it.

I wonder how many thieves have used this safe cracking technique with a pay phone and a stolen or invented credit card number?

[Although this is not computer related, it is symptomatic of back doors in many security systems. The manufacturer is probably smart enough to first verify that the credit card is legitimate, although it could have belonged to the owner of the house that was being burgled. However, if we assume that the owner had changed the default delivered combination, then this supposedly beneficial service would not help -- unless there was an unchangeable master combination IN ADDITION TO the user-set one. PGN]

⚡ Re: OpenBSD ... protects against buffer-overflow ... (Ardley, [R](#)

22.72)

Crispin Cowan <crispin@immunix.com>

Sat, 10 May 2003 19:19:12 -0700

>What is not so apparent is why technology that was developed
and operating
>over 30 years ago is just being re-invented in software.

Because what was developed in operating systems over 30 years
ago was use of
heavily segmented architectures. Over 20 years ago (the Intel
432) it was
discovered (the hard way) that such architectures run horribly
slowly
compared to RISC architectures. Since the debacle of the 432,
even CISC
processors such as the x86 have migrated towards RISC style
instruction
processing.

What OpenBSD is implementing is a variety of software schemes to
make up
for the lack of hardware protection for array bounds. Some of
these
schemes (Openwall's <<http://openwall.com/>> non-executable stack)
are
performance neutral: just mark the stack segment non-executable.
Some
(ProPolice, a re-implementation of StackGuard
<<http://immunix.org/stackguard.html>>) are very cheap
<<http://immunix.org/StackGuard/performance.html>>, much cheaper
than
enforcing memory safety in hardware.

Unfortunately, one of these enhancements (W^X) is not so cheap.
Here,
they try to make all writable pages non-executable, and vice
versa. This
is problematic on the x86 architecture because waaaay back in
the day,

Intel decided that memory pages did not need separate Read and Execute permission bits in the TLB (only segments have separate R and X bits, not pages). The W^X hack has to do a lot of work with TLB faults to compensate for this simple omission.

>The Burroughs 6700 implemented a hardware solution to the problem by
>assigning 3 bits of very 51 bit memory location to the type of data
>contained.

The 432 did something similar, and the performance penalty was astronomical. For a survey of buffer overflow attacks and defenses, check out these papers:

"Buffer Overflows: Attacks and Defenses for the Vulnerability of the Decade". Crispin Cowan, Perry Wagle, Calton Pu, Steve Beattie, and Jonathan Walpole. DARPA Information Survivability Conference and Expo (DISCEX) <<http://schafercorp-ballston.com/discex/>>, Hilton Head Island SC, January 2000. Also presented as an invited talk at SANS 2000 <<http://www.sans.org/sans2000/sans2000.htm>>, Orlando FL, March 2000. PDF <<http://immunix.com/%7Ecrispin/discex00.pdf>>.

"Software Security for Open Source Systems". Crispin Cowan. IEEE Security & Privacy Magazine <<http://www.computer.org/security/>>, February 2003, Volume 1, Number 1 <<http://www.computer.org/security/sp2003/jltoc.htm?SMSESSION=NO>>, pages 35-48. PDF <http://wirex.com/%7Ecrispin/opensource_security_survey.pdf>.

Crispin Cowan, Ph.D., Chief Scientist, Immunix <http://immunix.com>
<http://immunix.com/~crispin/> <http://www.immunix.com/shop/>

Re: OpenBSD ... protects against buffer-overflow ... (Ardley, R 22.72)

Dag-Erling Smorgrav <des@ofug.org>

Wed, 21 May 2003 10:27:23 +0200

I was rather disappointed to see that the attached e-mail, which I sent as a followup to Jeremy Ardley's comment on "OpenBSD release protects against buffer-overflow attacks" in 22.72, was not included in 22.73.

Jeremy Ardley made at least two serious factual errors: misidentifying the FreeBSD project (of which I am a member) with the OpenBSD project [*], and making incorrect assumptions (or wild guesses if you prefer) about Intel's IA32 architecture on the basis of the original article. My followup was intended to correct those errors and give RISKS readers a somewhat better understanding of the matter.

I was even more disappointed to see that 22.73 contained a further followup by Mike Albaugh which not only builds on Jeremy Ardley's incorrect assumptions about the IA32 architecture but furthermore does not (in my eyes) contain any useful information about any kind of RISK.

Dag-Erling Smorgrav - des@ofug.org

[* This error has been corrected in the SRI archive copy, and will be picked up in the risks.org Newcastle archive. PGN]

✶ Comment on BMW/MSFT failure reported in [Risks 22.73](#)

<john.opie@feri.de>

Wed, 21 May 2003 08:54:04 +0200

As someone who has professional ties to BMW (I work with Germany's largest private economic research group, which among other things provides the Quandt family - which own 48.1% of BMW - with investment advice) as well as having learned to drive on one (2002) and just order my third 5 (a 525td after a 530d and a 528i) series as a company car, there are a couple of points I'd like to make. I might be a tad biased 'cause I enjoy driving these cars so much (the 528i handled 240kmh with ease, but for fuel economy I will accept the top speed of 220 in the 525td...).

First, the 5 series does not use any MSFT products to run the car's systems. There are two Motorola PowerPC chips in the 5 series, one which runs the engine and the other takes care of the on-board electronics, which in turn run embedded systems that react to environmental changes (air conditioning) or to user changes (power windows, etc.). The on-board navigation system (getting one in the new car...) also uses an embedded, proprietary system.

Second, BMW 5-series cars include as a standard safety feature a

mechanical

interlock. If there is an accident or if there is an interruption of power lasting more than a few seconds, this interlock unlocks the doors in an event of an accident (determined by motion sensors and/or inflation of airbags), so that in case of locked doors and a driver accident which prevents the driver from unlocking the doors, rear-seat passengers are not trapped. They do not open the doors (there is an option for power-assisted door closing and opening...) but this does ensure that in case of accident, no one gets trapped. As a matter of fact, if there is an accident of enough severity to cause a set level of deformation in the motor cell, a small explosive charge will separate the battery of the car from the electrical system, preventing any electrical-caused fires in the wake of an accident.

Third, the new 7-series uses a version of WinCE for its I-drive. The new 5-series (with the Dr. Spock eyebrow blinkers) also uses a modified version of this as well. Both are heavily modified, for which BMW pays for. There is no reference to MSFT in BMW's advertising for the 7 series or the new 5 (at least I haven't seen any...)

But more fundamentally, and here is where risks come in, what should the default behavior of an armored limousine be? If I were to design such a system, the fundamental importance is to protect the passengers. If it became known that such an armored car would pop its locks when the on-board system would fail, then a terrorist/assassin/kidnapper could

exploit this in order to gain access to the passengers, either by an EMP trap or some other manner. Hence if the system failed on the BMW in question - which was most likely the 7-series armored limousine, which is the only armored limousine that BMW supplies (I think only in the 745 S and the 760 S versions with 4.5 V-8 and 6 liter V-12 engines with more horsepower than anyone else really needs) and which would be appropriate for the politician involved - it defaulted to the correct setup: protect the passengers.

John F. Opie, Feri Research GmbH, Haus am Park, Rathausplatz 8-10 D-61348 Bad Homburg von der Hoehe +49 (0)6172 916 3216 www.feri-research.com

✶ Spam's cure could be worse than the disease

"NewsScan" <newsscan@newsscan.com>

Tue, 27 May 2003 11:10:30 -0700

CNet columnist Declan McCullagh worries that the proliferation of spam-blocking software incorporating challenge-response technology could lead to the death of e-mail. Challenge-response systems require the human sending a message to perform a simple task such as clicking on a link or typing a special password to get past the barrier. The problem is, says McCullagh, that many challenge-response systems are poorly designed, and could causes big headaches for administrators of legitimate e-mail newsletters (such as NewsScan Daily) that go out to large

numbers of people. "Big corporations may be able to afford to hire someone to sit in front of a computer and spend all day proving they're not a spam bot, but nonprofit groups, individuals and smaller companies probably can't," says McCullagh. Earthlink has already announced its intentions to make a challenge-response system available to subscribers by the end of May, and other ISPs may follow suit -- a scenario that has veteran list operators concerned. Dave Farber, a computer scientist at the University of Pennsylvania who runs the "interesting people" list, says: "If I start getting a flood of challenges from Earthlink IPers that require my response I will most likely declare them spam and you will stop receiving IP mail. I fully expect this to be the case for almost all the legitimate mailing lists you are on and count on." Meanwhile, editors at the popular Macintosh newsletter TidBits, have told readers: "Be warned that we will not answer any challenges generated in response to our mailing list postings. Thus, if you're using a challenge-response system and not receiving TidBits, you'll need to figure that out on your own." [CNet News.com 27 May 2003; NewsScan Daily, 27 May 2003]

http://news.com.com/2010-1071_3-1009745.html?tag=fd_nc_1

✶ Spam limiting

Harry Hochheiser <hsh@cs.umd.edu>
Tue, 27 May 2003 09:54:08 -0400

Here's one that's either a risk or the most effective approach that I've yet seen for reducing/eliminating spam: simply refuse to accept any mail, even for your own host.

[Domain name and user changed to protect the innocent:]

The original message was received at Mon, 26 May 2003 12:49:34 - 0400 (EDT)
from localhost [127.0.0.1]

----- The following addresses had permanent fatal errors -----
<user@domain.com>

(reason: 550 5.7.1 <user@domain.com>... Relaying denied)

----- Transcript of session follows -----
... while talking to smtp2.domain.com:
>>> RCPT To:<user@domain.com>
<<< 550 5.7.1 <user@domain.com>... Relaying denied
550 5.1.1 <user@domain.com>... User unknown

✶ Re: more spelling-checker follies? (Hopkins, [RISKS-22.73](#))

"Anna Shefl" <anna@ledsafetyhazard.net>

Wed, 21 May 2003 09:55:30 GMT

> For three minutes, an AP story posted on *The New York Times* Web site about
> Justice Clarence Thomas referred to his predecessor as "Turgid Marshall."

MS has also made the historical black leader Marcus Gravy famous. Given how many names are not spelling-checker-friendly, I'm all the more surprised at how many people let spelling-checkers run on auto-pilot. We'll

have to wait

and see what risks, other than embarrassment, could occur as a consequence.

I searched the Web for "Osaka bin Laden". Results 1 - 40 of about 70.

REVIEW: "Protected Internet, Intranet, and Virtual Private Networks",

Rob Slade <rslade@sprint.ca>

Tue, 20 May 2003 14:00:51 -0800

Alexander Moldovyan et al.

BKPIIVPN.RVW 20030404

"Protected Internet, Intranet, and Virtual Private Networks",
Alexander Moldovyan et al., 2003, 1-931769-14-1, U\$44.95/C\$67.95

%A Alexander Moldovyan

%A Nick Moldovyan

%A Doug Summerville

%A Vladimir Zima

%C 295 East Swedesford Road, PMB #285, Wayne, PA 19087

%D 2003

%G 1-931769-14-1

%I A-LIST LLC

%O U\$44.95/C\$67.95 fax 702-977-5377 mail@alistpublishing.com

%O <http://www.amazon.com/exec/obidos/ASIN/1931769141/>

[robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/1931769141/robsladesinterne)

<http://www.amazon.co.uk/exec/obidos/ASIN/1931769141/>

[robsladesinte-21](http://www.amazon.co.uk/exec/obidos/ASIN/1931769141/robsladesinte-21)

%O <http://www.amazon.ca/exec/obidos/ASIN/1931769141/>

[robsladesin03-20](http://www.amazon.ca/exec/obidos/ASIN/1931769141/robsladesin03-20)

%P 310 p.

%T "Protected Internet, Intranet, and Virtual Private Networks"

Despite the slim size, it is still disconcerting to find that there are only

three chapters in this book. Chapter one provides an introduction to client/server networking, while implying that the technology is **not** hierarchical. Basic networking concepts are covered, but the writing has an academic pomposity without the requisite rigour. Figures and illustrations are not only unhelpful, but may actually confuse issues, and typographical and grammatical errors abound. Lists of idiosyncratic, and very odd, attack taxonomies are given in chapter two. Items like "attacks on the security policy and administration procedures" aren't really explained, while "attacks on permanent components of the security system" seems to be limited to cryptanalysis. Chapter three has some descriptions of virtual private networks, tunnelling, IPSec, and key management protocols.

The writing is hard to understand, there does not seem to be any logical organization to the material, and the mistakes in the content do not inspire any confidence in the reliability of any part of this text. All the topics touched on here are covered much more effectively in other works, but the topics are so random that it is difficult to make specific recommendations.

For those interested in the basics of data communications I would suggest Tanenbaum (cf. BKCMPNWK.RVW), while "Building Linux Virtual Private Networks (VPNs)" (cf. BKBLVPNS.RVW) is a good introduction to VPNs themselves.

copyright Robert M. Slade, 2003 BKPIIVPN.RVW 20030404
rslade@sprint.ca rslade@vcn.bc.ca slade@victoria.tc.ca
pl@canada.com

✦ Survivable and Self-Regenerative Systems: workshop

Doug Maughan <dmaughan@darpa.mil>

Thu, 22 May 2003 02:34:26 -0400

2003 ACM Workshop on Survivable and Self-Regenerative Systems
In conjunction with
2003 ACM International Conference on Computer and
Communications Security
(CCS-10)

31 Oct 2003

George W. Johnson Center at George Mason University, Fairfax,
VA, USA

Call for papers

One of the key areas of current research in the fields of computer and communication security is survivability, where the objective is to survive rather than to prevent or detect intrusions. Survivability research has explored the intersection of Fault Tolerance and Security, and recently, the notion of using self-regenerative capabilities in the context of survivability has generated a significant interest in the community. This workshop aims to provide a venue for scholars in this area to exchange ideas and to explore research issues involving survivable and self-regenerative systems. Papers offering original research contributions in any aspect of this emerging field are solicited for submission to this workshop.

Topics of interest include, but are not limited to, the following:

- * Survivable Systems & Networks
- * Self-Regenerative Systems & Networks
- * Use of Self-Healing Techniques in Surviving Attacks
- * Security vs. Fault Tolerance in building survivable and self-regenerative systems
- * Use of Self-Stabilization Techniques in Surviving Attacks
- * Role of Formal Models in Survivable and Self-Regenerative Systems
- * Self-Adapting and Self-Securing Systems and Techniques
- * Measuring and Quantifying Survivability and Self-Regeneration
- * Role of Redundancy, Diversity, Unpredictability and Deception in Survivable and Self-Regenerative Systems
- * Impact of Detection Accuracy and Latency on Survivability and Self-Regeneration

Papers due: July 9, 2003

Link to the workshop can be found from the CCS webpage at:

<http://www.acm.org/sigs/sigsac/ccs/CCS2003/>



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

[ACM](#) Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 75

Friday 30 May 2003

Contents

- [Algeria earthquake cuts Internet connectivity of major Greek ISP](#)
[Diomidis Spinellis](#)
- [Diving computer flaw allegedly covered up](#)
[Craig S. Bell](#)
- ["Computer glitch" causes false dam failure warning](#)
[Rich Mintz](#)
- [ISP resets password to an easily guessed one](#)
[Dawn Cohen](#)
- [Ballot scanning problems in New York City](#)
[Doug Kellner](#)
- [Sensitive data on Web sites reflects lack of security awareness](#)
[Rick Weiss](#)
- [Re: OpenBSD ... protects against buffer-overflow](#)
[Paul Karger](#)
- [Re: Modern Computers, Unsafe at any speed?](#)
[Bill Stewart](#)
- [Re: BMW/MSFT failure reported](#)
[Geoff Kuenning](#)
- [No call list preventing 911 notifications](#)
[Robert Franchi](#)

- [University of Calgary going to teach virus writing](#)
[Klaus Brunnstein](#)
 - [REVIEW: "Hack Attacks Testing", John Chirillo](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ **Algeria earthquake cuts Internet connectivity of major Greek ISP**

Diomidis Spinellis <dds@aueb.gr>

Fri, 23 May 2003 12:45:32 +0300

OTEnet, the Greek ISP associated with the incumbent telephone operator, appears to be cut off from the (non-Greek) Internet for almost two consecutive days, due to damage from the Algerian earthquake. According to a note on their home page (<http://www.otenet.gr/> - May 23rd - in Greek), the May 21st Algerian earthquake damaged a number of international cables (Flag, SMW2, SMW3, Columbus2) that passed through the area, cutting-off OTEnet's international IP connectivity. Dial-up customers are advised to use their Web proxy server as a temporary measure.

A different page <<http://www.otenet.gr/company/whyus.htm>> boasts that OTEnet's network is the largest and most important [sic] Greek network featuring 65 points of presence, a 155Mbps backbone, a 100Mbps peering connection, and 310Mbps international connections. Apparently physically redundant international connections or peering agreements that would cover such an emergency were not foreseen.

A number of Greek companies serviced by the particular ISP appear also to be cut off. Other ISPs and the Greek academic network were not affected, probably because they depend on different cables. The risk? Although IP technology supports the rerouting of packets around failed links, short-sighted network deployment architectures and peering agreement practices often fail to exploit this capability.

Diomidis Spinellis - <http://www.dmst.aueb.gr/dds>

✶ Diving computer flaw allegedly covered up

"Craig S. Bell" <craig@runbox.com>

Tue, 27 May 2003 04:14:06 GMT

I am not a diver, myself; however, I found this story somewhat alarming. This report discusses a lawsuit surrounding the alleged coverup of serious problems with a certain Aladin diving computer, beginning in 1995. The safety of Aladin diving computers was discussed in [RISKS 7.60](#), several years before this particular product debuted.

<http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2003/05/25/MN309974.DTL>

Summary: If you make several short dives in relatively quick succession, the Aladin Air X Nitrox may dangerously overestimate how much dive time you have remaining.

The primary risk is conventional: Despite reports of serious injury, the Swiss company's two founders successfully covered up knowledge of this flaw for seven years. This subterfuge overcame the efforts of some within the company to recall the defective computer, or otherwise make the public aware of the problem.

⚡ "Computer glitch" causes false dam failure warning

Rich Mintz <richmintz@richmintz.com>

Fri, 23 May 2003 12:39:29 -0400

A "computer glitch" at Santee Cooper, the quasi-public agency that operates dams and power generation facilities in the South Carolina lowcountry, resulted in the broadcast of a false public warning that the Santee Dam on Lake Marion had failed. Apparently, a flood watch went out electronically at 3:16 AM, and then the sirens and loudspeakers began broadcasting a verbal warning of dam failure throughout the area about 8:30 AM. A Santee Cooper spokesman said, "A computer program kicked in gear that wasn't supposed to kick in gear," he said. "We're trying to get our arms around what caused this so it doesn't happen again." Santee Cooper also noted that not all the sirens that should have gone off in such a scenario actually went off, which is a separate problem they are investigating.

The Santee Dam, which is part of the Santee Cooper lake system comprising

Lakes Marion and Moultrie, is just upriver from the city of St. Stephen, about 50 miles NW of Charleston, in a region supported by fishing and lake tourism but also increasingly suburbanized. U.S. 52 connects the area to Moncks Corner and Charleston. From the article:

>The threat of a dam break is no laughing matter on the Santee. Engineers estimate that the wave from a collapse would hit the U.S. Highway 52 bridge in four hours. After eight hours, that bridge would be submerged by a river level 25 feet above normal, and 14-foot floodwaters would have reached St. Stephen. The flood would reach the sea within 48 hours.

From the Charleston (South Carolina) Post & Courier:

http://www.charleston.net/stories/052303/loc_23dam.shtml.

Detailed lake maps:

<http://www.santeecooper.com/environment/recreation/lakemaps.html>

Santee Cooper press release:

http://www.santeecooper.com/aboutus/newsroom/releases/news_2003_0522.html

Thanks to Wes Singletary for the referral.

ISP resets password to an easily guessed one

"Dawn Cohen" <COHEND@wyeth.com>

Fri, 23 May 2003 10:14:58 -0400

Here's one from the I-can't-believe-they-would-do-such-a-thing department.

Our local broadband provider was RCN, but due to various

mismanagement or economic issues, was essentially ousted by our community. The service was picked up by Patriot Media, which doesn't seem to be doing much better.

We were notified around the same day as the switchover took place that e-mail accounts would be changing to the <old-user-name>@patmedia.net, though we would have a grace period of a couple of months to transition.

My husband tried to log in to his e-mail this morning, and couldn't manage to get in. After I turned the switch on for him (:-) he still couldn't get on, and after a lengthy wait for access to a Patriot Media customer service person, he found out that his user name had been changed to his old user name with a "1" appended, and his password had been reset to "rcnrncn".

Need I say more?

✶ Ballot scanning problems in New York City

Doug Kellner <dkellner@boe.nyc.ny.us>

Thu, 22 May 2003 14:49:42 -0400

The NYC Board of Elections' system for scanning absentee ballots miscounted at least 19 ballots in a recent closely contested special election for a city council seat apparently because the scanner improperly sensed the blank voting oval. Because the voters had properly marked another oval, the

computer voided the ballots as overvotes.

<http://www.vote.nyc.ny.us/pdf/documents/boe/ReportOnTheScanningOfPaperBallots.pdf>

Douglas A. Kellner, Commissioner, Board of Elections in the City of New York
200 Varick Street, New York, New York 10013 Tel. (212) 889-2121

[This is not the first time I have heard of a blank oval being detected
as over threshold for a marked oval. Just one more risk! PGN]

✶ Sensitive data on Web sites reflects lack of security awareness

Rick Weiss <rickw4s@yahoo.com>
Thu, 29 May 2003 11:06:34 -0700 (PDT)

My health insurance contracts with PrecisionRX.com for lower-cost prescription drugs. I recently wanted to order refills, and found that they had changed their Web site, and that I needed to register to be able to order refills. The registration process was mostly just me authenticating myself.

The next day I received 2 e-mail messages from PrecisionRX.com (sent 5 seconds apart). One said "your username is blah". The other: "your password is blah". Each said that they were sent separately for security purposes.

So I logged in. The login process ONLY required the username and password

--- no other authentication was required for that first login!
And I wasn't
forced to change my password. In fact, there was no ability to
change my
password.

Once logged in, I (or anyone who intercepted the e-mail) could
view my full
name, address, birth-date, social security number, doctors'
names,
prescriptions etc. Not only are they putting my identity at
risk of theft,
but they are violating HIPAA too (by not taking reasonable steps
to keep
others from viewing my private information).

After complaining alot, they put me in touch with their head of
IT, David.
David told me that their system (e-mailing both username &
password without
any protection, not requiring further authentication to login,
not requiring
immediate password change) was indeed secure, and accepted
practice too!

[✶ Re: OpenBSD ... protects against buffer-overflow \(Cowan, RISKS-22.74\)](#)

<karger@watson.ibm.com>

Thu, 29 May 2003 12:46:53 -0400

This is a long comment, but I think it is very important to
correct
some myths about segmentation hardware. I have removed some of
Crispin Cowan's text to make this shorter, and I hope that in
doing
so, I didn't change the intent of his remarks. If I did, please
accept my apology in advance!

>>What is not so apparent is why technology that was developed and operating
>>over 30 years ago is just being re-invented in software.

>Because what was developed in operating systems over 30 years ago was use of
>heavily segmented architectures. Over 20 years ago (the Intel 432) it was
>discovered (the hard way) that such architectures run horribly slowly
>compared to RISC architectures. Since the debacle of the 432, even CISC
>processors such as the x86 have migrated towards RISC style instruction
>processing.

Crispin Cowan's remarks that the Intel 432 had horrible performance are absolutely correct. Unfortunately, the horrible performance had absolutely NOTHING to do with the segmentation architecture, and his conclusion to avoid segmentation is incorrect.

The performance lessons of the Intel 432 are EXTREMELY important for anyone in the OS or security field to learn, both to see what was an utter failure on that machine as well as what was NOT an utter failure! The following two references cover these lessons extremely well. Please pardon the BibTeX syntax.

```
@article{colwell:controversy,  
  author = "Colwell, Robert P. and {Hitchcock III},  
Charles Y. and  
          Jensen, E. Douglas and Brinkley Sprunt, H.M.  
and  
          Kollar, Charles P.",  
  title = "Computers, Complexity, and Controversy",  
  journal = "Computer",
```

```
volume = 18, number = 9, month = sep, year = 1985, pages  
= "8--19" }
```

```
@phdthesis{colwell:phd,  
  author = "Colwell, Robert P.",  
  title = "The Performance Effects of Functional Migration  
and  
          Architectural Complexity in Object-Oriented  
Systems",  
  type = "Ph.D. thesis",  
  school = "Department of Computer Science, CMU-CS-85-159,  
          Carnegie-Mellon University",  
  address = "Pittsburgh, PA, USA", month = aug, year =  
1985 }
```

It is indeed true that that x86 architecture was designed to be used with segmentation, and almost all operating systems that have been written for it do NOT use the segmentation. It is also true that on the x86 that execute protection without segmentation is a royal pain. But this does not mean that using execute protection hardware is bad or that segmentation is bad. It only means that the x86 is badly designed for operating systems that do not use segmentation. The GEMSOS operating system (the only system that I know of to use x86 segmentation) uses that kind of execute protection with very good performance! Operating systems that don't use segmentation need to have read, write, and execute permission bits on every page of memory. If you don't have that, you will have trouble!

By the way - I think Crispin's work on solving buffer overflows on x86 to be very good. I am NOT criticizing that work at all - only the generalization that segmentation is bad in all cases.

>>The Burroughs 6700 implemented a hardware solution to the problem by
>>assigning 3 bits of very 51 bit memory location to the type of data
>>contained.

The Burroughs B6700 (still sold by Unisys as the A-series today) is a good example of how to use segmentation in an operating system and get very good performance as well as very good buffer overflow protection. Multics did exactly the same thing to great success. See my paper:

Karger, P.A. and R.R. Schell. Thirty Years Later: Lessons from the Multics Security Evaluation. in Proceedings of the 18th Annual Computer Security Applications Conference. 2002, Las Vegas, NV IEEE Computer Society. p. 119-126. URL:
<http://www.acsac.org/2002/papers/classic-multics.pdf>

>The 432 did something similar, and the performance penalty was >astronomical.

Colwell's papers make very clear that the horrible performance penalties on the 432 did NOT come from segmentation. They came from several other bad ideas including allowing instructions to start on arbitrary bit boundaries making instruction decode extremely hard, using full cross-domain calls for EVERY subroutine call, and numerous other performance atrocities.

In addition to the Burroughs 6700 and Multics, the IBM System 38, AS/400, and iSeries servers all use segmentation and capabilities to great success. For segmentation to be useful, you have to have LOTS of segments in the architecture and each segment must be large enough. The 80286 chip didn't

have either enough segments or big enough segments, and that started the myth that segments were bad. The 80386 pretty much fixed those problems. Multics segments were only 1 megabyte in size, and that was known to be too small all the way back in 1970! My personal opinion is that for a segmented architecture to succeed, you would need at a minimum 64K of segments, with each segment allowed to grow to at least 4gigs. Of course bigger numbers would be preferable, and with 64-bit processors today, that is not a problem. The IBM AS/400 and iSeries have (I think - I might have this wrong) 128-bit addresses!

So in conclusion -- segments are most definitely not evil! Only badly designed segments are evil! It is important to design operating systems that work the same way that the hardware designers intended. If you don't do that, and on the x86, almost no one has done that, then you will have problems. That is part of why we suffer from buffer overflows today. There are lots of other reasons as well, of course. The C programming language is certainly another very big culprit. Almost any other language is better than C when it comes to buffer overflows - even FORTRAN!

One final comment - segmentation can give a lot of security benefits, but segmentation is not the one and only true way - just as I believe that segmentation is not inherently bad, it is also the case that you can get most of the same benefits with a non-segmented machine IF you have the right protection bits on every page. My point is that it is crucial

to have a
match between the CPU architecture and the OS architecture, and
we don't
have that on the x86 for almost all operating systems available
today.

Paul A. Karger, Ph.D., Cantab., IBM, T. J. Watson Research Center

[A subsequent response from Crispin and Paul's response to that
are not included herein, That discussion was very interesting
to
me personally (as an old Multician), but probably of less
interest
to RISKS readers generally. PGN]

⚡ Re: Modern Computers, Unsafe at any speed?

Bill Stewart <bill.stewart@pobox.com>

Thu, 29 May 2003 02:31:35 -0700

I was startled by "Len Spyker" <redmond2@iinet.net.au>'s
assertion in
[RISKS-22.74](#) that "all that software now wasting CPU time
checking for
overflows is no longer needed" because hardware can protect us
against
overflows.

Hardware can't protect you against wrong answers, and while it
can detect
some kinds of overflows and halt a program rather than let it
dangerously
stomp on other space, that isn't always the right way to respond
to a
problem - you might want to do other things like giving the user
or
administrator an error message rather than stopping.

Also, hardware protection against stack overflows is easier than protection against overflows of individual arrays that don't go outside the segment, and setting up protection for arrays, at least on most hardware, is a lot more work. Yes, this will generally stop many kinds of potential security attack.

But back in the mid-70s, when I was learning to program well in college (as opposed to learning to program haphazardly in high school), one of the first and most critical lessons was to always check your program's input and **never** trust it. It might be bad input by accident, or malicious input on purpose, and the input data we had to run our class programs on was always malicious, particularly designed to catch off-by-one errors, which are a common problem with arrays. Empty-input errors are fun too, and are often caused by input data that's out of sync, or by input data that's the wrong type (e.g. letters when you need numbers.)

Some computer languages will help a lot with bounds checking, while others, like C, will let you shoot yourself in the foot, though they make it hard to shoot somebody else in the foot. Cornell's PL/C compiler (for their dialect of PL/I) not only detected syntax errors, it tried to correct them. Sometimes it did it right, sometimes it did it wrong, but it at least let you try to run the program so you could find as many bugs per set of keypunch exercise as possible.

⚡ Re: BMW/MSFT failure reported (Opie, [RISKS-22.73](#))

<geoff@cs.hmc.edu>

Wed, 28 May 2003 22:40:06 -0700 (PDT)

Perhaps I'm clueless for only owning a cheap Toyota, but on my car, I'm not stuck depending on electronics (and their associated power) to lock and unlock the doors. The power locks are only an assist. No matter what a terrorist does, I can hand-operate the mechanical locks in either direction.

The true RISK is falling so in love with computerization and power assists that one forgets simple, reliable design. Doors that open themselves? Unless you're severely disabled, give me a break.

Geoff Kuenning geoff@cs.hmc.edu <http://www.cs.hmc.edu/~geoff/>

[Przemek Klosowski recalled the old chestnut about the thief drop-kicking

the collision/deceleration sensor, which deploys the airbags and opens

the car doors. Just a reminder. PGN]

⚡ No call list preventing 911 notifications

"Franchi, Robert" <Robert.Franchi@fmr.com>

Fri, 30 May 2003 11:21:33 -0400

[http://www.boston.com/dailyglobe2/149/northwest/
Call_blocking_may_be_safety](http://www.boston.com/dailyglobe2/149/northwest/Call_blocking_may_be_safety)

[risk+.shtml](#)

<<http://www.boston.com/dailyglobe2/149/northwest/>

[Call blocking may be safety](#)

[_risk+.shtml>](#)

People who are on the MASS "Do not Call" list were also not included on the 911-emergency notification list (for emergency evacuations etc.). Apparently, the company that provides the list to the Massachusetts 911 system, Reverse 911, uses commercially available lists that have already had "Do Not Call" list people removed.

Bob Franchi, FB&RS-Tech FTPS Accounts - Merrimack (603) 791-5833

✶ University of Calgary going to teach virus writing

"Klaus Brunnstein" <brunnstein@informatik.uni-hamburg.de>

Fri, 30 May 2003 15:18:01 +0200

RF readers are well aware about many cases where malicious code (aka viruses, worms, trojans) has adversely influenced proper work in enterprises and organisations. It may therefore come as surprise that a renown Canadian university - University of Calgary - is going to teach how to write viruses:

http://www.cpsc.ucalgary.ca/News/virus_course.html

This Web page is a result of rather controversial disputes in several fora which lead the department to rephrase their earlier announcement which revealed the reason for the course in full naivety. I quote (without

permission) from UoCs earlier Web site (after a paragraph quoting experts on damage of malware):

"Dr. John Aycock, professor for this course, convinced the Department to support his idea for offering a course in this area. He says that in order to develop more secure software, and countermeasures for malicious software, you first need to know how malicious software works and the mindset of its creators. By looking through the eyes of the people who develop these viruses, our students will learn what their targets actually are and what needs to be protected. It's a case of being proactive rather than reactive. This attitude is similar to what medical researchers do to combat the latest biological viruses such as SARS. Before you can develop a cure, you have to understand what the virus is and how it spreads - why should combating computer viruses be any different?"

As far as I understand biologists, they DO NOT generate new viruses but try to extract parts of existing virus code to develop countermeasures. In Informatics, the equivalent technique is called "Reverse Engineering". Indeed, you can analyse malicious code WITHOUT THINKING LIKE A VIRUS AUTHOR, as Dr. Aycock and his faculty seem to think.

Of course, there have been biologists, chemists and physicists who developed - "proactively" - some new specimen of related kinds but their goal was NOT to protect humankind but to the contrary to develop new weapons. In the Information Society, malware are weapons against those

institutions which depend upon proper work of IT. In order to defend against such weapons, one must NOT THINK as attacker but in terms of the attacked.

In this sense, it is UNETHICAL (if not yet illegal in some parts of the world) to write viruses.

Now, UoC includes discussions of ethics in their course. As if this makes the dubious goal more honorable: it is inherently "unethical" to write malicious code. The inclusion of some paragraphs of ethics in UoC course is no more than an alibi.

After 15 years of teaching how to detect, cure and possibly prevent malicious code in my courses at Hamburg university since 1988), I have NEVER seen any need nor has any of my students wished to write harmful code. Instead, we teach Reverse Engineering (which is legal for purposes of defense in Germany).

My hope is that University of Calgary experts instruct their students in methods how to detect, cure and prevent contemporary IT rather than wasting times in teaching methods how to potentially generate harm.

Klaus Brunnstein (Faculty for Informatics, University of Hamburg)

⚡ REVIEW: "Hack Attacks Testing", John Chirillo

Rob Slade <rslade@sprint.ca>

Thu, 29 May 2003 14:19:02 -0800

BKHKATTS.RVW 20030330

"Hack Attacks Testing", John Chirillo, 2003, 0-471-22946-6,
U\$50.00/C\$77.50/UK#34.95

%A John Chirillo

%C 5353 Dundas Street West, 4th Floor, Etobicoke, ON M9B 6H8

%D 2003

%G 0-471-22946-6

%I John Wiley & Sons, Inc.

%O U\$50.00/C\$77.50/UK#34.95 416-236-4433 fax: 416-236-4448

%O <http://www.amazon.com/exec/obidos/ASIN/0471229466/>

[robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/0471229466/)

<http://www.amazon.co.uk/exec/obidos/ASIN/0471229466/>

[robsladesinte-21](http://www.amazon.co.uk/exec/obidos/ASIN/0471229466/)

%O <http://www.amazon.ca/exec/obidos/ASIN/0471229466/>

[robsladesin03-20](http://www.amazon.ca/exec/obidos/ASIN/0471229466/)

%P 540 p. + CD-ROM

%T "Hack Attacks Testing"

The description in the introduction seems to indicate that this text

might be similar to SATAN (Security Administrator's Tool for Analyzing

Networks), in that it explains how to build a set of utilities in order to identify vulnerabilities. As such, there is the possibility

that the work is open to a charge of being more useful to attackers

than to defenders. Fortunately, the book does not provide a great

deal of information that could be used to break into systems. Unfortunately, it doesn't help much with defence, either.

Part one is supposed to describe how to build a multisystem "Tiger

Box," similar to SATAN, and the overview outlines the components of a

penetration test. Chapters one to four, however, simply narrate the

installations for Microsoft Windows NT and 2000, Red Hat Linux, Solaris, and Mac OS X, using the installation programs provided. The

material is heavy on screen shots, and light on explanations of what is going on and why. There is no provision for specific security testing requirements, or even multiboot systems.

Part two lists penetration analysis tools for Microsoft Windows, and the introduction tabulates common vulnerability classes. Chapter five explains how to install the Cerberus Internet scanner, enumerates the possible reports, and gives one (eight page) sample report. Much the same is true for the Cybercop Scanner, Internet Scanner, Security Threat Avoidance Technology (STAT), and TigerSuite products in chapters six through nine. All of these systems do multiple probes and analysis.

The description of UNIX and OS X tools, in part three, starts with a twenty page list of UNIX commands. UNIX utilities tend to be more single purpose: hping/2 is for IP spoofing and nmap is for port scanning, but Nessus, SAINT (Security Administrator's Integrated Network Tool), and SARA (Security Auditor Research Assistant) are collections.

Part four is entitled "Vulnerability Assessment," but contains only chapter fifteen, which contains checklists for securing various systems, primarily relying on outside sources.

Despite the introduction, this book does **not** describe how to set up a "Tiger Box." It lists a few vulnerability scanners and utilities. There is little in the way of help or explanations, and the material seems to be based primarily on product documentation and commonly available guides. The content actually by Chirillo often seems so oddly written that it is difficult to parse any meaning from the

text.

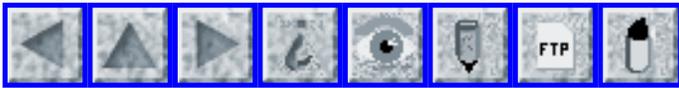
The book does provide you with a list of vulnerability scanners. But then, so would any decent Web search.

copyright Robert M. Slade, 2003 BKHKATTS.RVW 20030330
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca
pl@canada.com

<http://victoria.tc.ca/techrev/~rslade> or <http://sun.soci.niu.edu/~rslade>



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 22: Issue 76

Friday 13 June 2003

Contents

- [Challenge to 'challenge-response' users: Be Careful!](#)
[NewsScan](#)
- [Phantom voting in Israeli Knesset](#)
[Ed Ravin](#)
- [Student hacks school, erases class files](#)
[PGN](#)
- [Canadian firearm registration system overwhelmed by traffic swabsox via Declan McCullagh](#)
- [Sea King Helicopter crash - fire control system deployment failure](#)
[Stuart Lynne](#)
- [Computer glitch causes traffic lights malfunction](#)
[Teemu Leppänen](#)
- [Risks of trusting CORRECT dive computers and tables](#)
[Daniel P.B. Smith](#)
- [Electric utility direct-debit fiasco](#)
[Jonathan Kamens](#)
- [Incremental insecurity](#)
[Paul Wexelblat](#)
- [Re: ATM time sync](#)
[David Leshner](#)
- [Re: University of Calgary to teach virus writing](#)
[Nicholas Weaver](#)
[Dan Bornstein](#)

- [Denial of Service via Algorithmic Complexity Attacks: Crosby-Wallach](#)
[Monty Solomon](#)
 - [REVIEW: "Mission Critical Security Planner", Eric Greenberg](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Challenge to 'challenge-response' users: Be Careful!

"NewsScan" <newsscan@newsscan.com>
Mon, 09 Jun 2003 10:01:34 -0700

EarthLink has begun offering its 5 million subscribers "challenge and response" technology set up to send a "challenge" to any message from an unknown source, requiring that source to "respond" (and thereby supposedly proving it's from a human being rather than a spammer or pornographer). But many people who hate spam are saying the cure is worse than the illness; anti-spam consultant Steve Adkins warns, "It's sufficiently tempting that people will use it and will not realize all the bad things that will begin happening. Challenge-response is very, very unfriendly and rude to legitimate senders of e-mail." [AP/*Seattle Post-Intelligencer*, 9 Jun 2003; NewsScan Daily, 9 June 2003]
http://seattlepi.nwsource.com/business/125638_spamtech06.html

[Note: If you sign up for challenge-response, then say goodbye to NewsScan Daily. (The NewsScan editors)]

[And say goodbye to RISKS also (unless you set up an alias address for RISKS issues that does not challenge. (We will never reveal it.) PGN]

✶ Phantom voting in Israeli Knesset

Ed Ravin <eravin@panix.com>

Wed, 4 Jun 2003 17:44:15 -0400

An investigation is going on in the Israeli Knesset (Parliament) on how votes are being cast on behalf of parliamentarians who are absent from their seats. It seems that electronic voting has problems even in a controlled environment like the floor of a parliament...

Knesset probe fails to reveal who voted in Likud

By Gidon Alon, Haaretz Correspondent

A special committee set up by Knesset Speaker Reuven Rivlin, has failed to

discover which MK was responsible for voting in place of Likud MK Inbal

Gavrieli, who was not present in the Knesset plenum during a debate concerning the new budget plan, even though computer records indicate a

vote was cast from her seat.

Israel Radio reported several Likud MK's saying they had observed MK Yehiel Hazan (Likud) voting on Gavrieli's behalf. The vote was conducted electronically.

The incident follows another case of double voting, in which MK Michael

Gorlovski (Likud) admitted to having voted on behalf of another Likud MK,

Gilad Erdan, also during the vote on the economic plan.

<http://www.haaretzdaily.com/hasen/pages/ShArt.jhtml>

?

itemNo=300587&contrassID=1&subContrassID=7&sbSubContrassID=0&listSrc=Y

✶ Student hacks school, erases class files

<neumann@csl.sri.com>

Thu, 12 Jun 2003 08:35:00 -0400

A 17-year-old student in a networking course was arrested for breaking into his school's computers and erasing folders of other members of the junior class at Marion High School, near Rochester NY. He apparently was sniffing passwords with keylogging software. [The school's fix for this is to have students change their passwords every 60 days, and force them to use passwords with a ``combination of letters, numbers, and at least one special character''. Whoopee! That sure solves the problem! Sure stops the sniffer, which could be getting the new passwords as they are entered!!! PGN]

<http://www.cnn.com/2003/TECH/internet/06/10/school.hacked/index.html>

[One of our correspondents suggested that perhaps his charges will claim that his keylogging software is in the WMD category, and ask for a life sentence. PGN]

Canadian firearm registration system overwhelmed by traffic

Declan McCullagh <declan@well.com>

Fri, 06 Jun 2003 09:43:26 -0400

>Date: Fri, 6 Jun 2003 08:41:33 -0600
>From: swabsox <swabsox@knology.net>
>To: Declan McCullagh <declan@well.com>
>Subject: ITBusiness.ca

>
>Gun registry backfires after system exceeds capacity:

>
> The CFC's IT woes really aren't that different from any other government

>department's, said Wendy Cukier, president of the Toronto-based
Coalition for
>Gun Control. She noted that government projects are frequently
plagued by
>things like budget and capacity issues, but the amount of vocal
opposition to
>the gun registry and made the CFC a flashpoint for controversy.
>
>"The system was built on the assumption that it would have something
like
>a 10% error rate and instead the error rate was 90 per cent. Some of
that
>was because of the complexity of forms and some of that was
deliberate" said
>Cukier, who's also a professor of information technology management
at
>Ryerson University. "You'd be hard-pressed to find another program
that faced
>such extensive efforts to undermine it."
>
><http://www.itbusiness.ca/index.asp?theaction=61&lid=1&sid=52538>

✈ Sea King Helicopter crash - fire control system deployment failure

Stuart Lynne <sl@belcarra.com>
Wed, 4 Jun 2003 21:24:27 -0700

An article in today's *National Post* related that, when a Sea King helicopter crashed on the deck of a Canadian Forces Iroquis destroyer earlier this year, the first two fire control systems failed and only the third finally worked.

The article does not say why the first system failed, but the second failed because of an obviously (well, perhaps in hindsight, obvious to RISKS readers) poor design of the operators console:

An operator in the control room then pressed a button to active the second system. Nothing seemed to happen. He pushed the button again and

again --

a total of six times -- but nothing happened.

The operator "was not aware of the fact that as he repeatedly depressed

the button to activate the AFFF system, he was actually starting and stopping the system with every alternate push," a report from the subsequent technical investigation says.

It also notes none of the indicator lamps on the system's console were

working, so they did not light up when the button was pushed.

And the crew may not have known about a 30-second delay from the the system is activated to the time the fire suppressant reaches the hose

nozzle...

1. Poor design of a critical system. A toggle or second switch to disarm would have been a better choice perhaps.

2. Poor maintenance apparently leaving a critical system usable but not apparently so when the operator wanted results right now.

3. Poor training so that the operator did not know what to expect when activating the system.

Kudos that they did have a third fire control system that apparently was deployed successfully.

Stuart Lynne <sl@belcarra.com>

Belcarra, Embedded Linux USB Software 604-461-7532

🔥 Computer glitch causes traffic lights malfunction

Teemu Leppänen <teemulep@sun3.oulu.fi>

Sat, 31 May 2003 11:25:24 +0300 (EEST)

In Oulu, Finland, computer glitch in central "traffic lights controlling"

computer caused traffic jams in city centre at 9am friday morning. The computer transferred back to year 1991 and to night time (they did not specify exact date and time), meaning some of the traffic lights were in

"night mode" and signaling "ignore me". Problem was solved in 90 minutes,

but the original cause of the glitch remains yet unknown. Authorities say

this was the first glitch ever experienced by the tax payers, also admitting

there has been "minor" ones before. Seems that the police was not used to

guide the traffic instead.

No accidents were reported, hence no need to clear the way for the emergency

medical teams.. perhaps with system which state is unknown, even requiring

reboot, or having technicians trying to fix the issue at the same time.

Original article (in Finnish) <http://plus.kaleva.fi/html/JTpage321980.html>

✦ Risks of trusting CORRECT dive computers and tables

"Daniel P.B. Smith" <dpbsmith@bellatlantic.net>

Fri, 30 May 2003 23:15:39 -0400

Craig S. Bell submitted a note about dive computers with an alleged software

defect. Without minimizing the seriousness of the issue, or excusing the

alleged behavior of the manufacturer, I think there is another RISK as well.

The actual physiology and physical chemistry of decompression sickness isn't

understood precisely. The models used to calculate dive tables and

those
used in dive computers are rough.
<http://www.theage.com.au/articles/2002/12/11/1039379882081.html>
cites a Dr. Gregory Emerson as saying, of decompression sickness, "We
kind
of know why it occurs but we still don't really understand why some
people
get it and other people don't."

A manual I downloaded from <http://www.uwatec.com> says that "Aladin Pro
Nitrox uses a new decompression calculation model known as the ZH-L8
ADT. This model uses eight compartments or 'tissue' groups with
nominal half
time periods from 5 to 640 minutes." In another place, however, they
make
the disclaimer "decompression modeling is an inexact science, and of
necessity must be based at least partly on certain unproven
assumptions."
(I interpret this to mean that their "eight-compartment ZH-L8 ADT
model" can
be regarded as an educated guess).

But even if the model were perfect, it would not be perfectly accurate
unless there were a way to measure the size of an individual diver's
tissue
"compartments." The manual makes no reference to any way of matching
the
device to the body characteristics an individual diver. There is no
way to
enter percentage of body fat, for example, let alone the other seven
tissues
incorporated in the model.

And nitrogen is soluble in fat. A person with more body fat will
absorb
more nitrogen while breathing compressed air at depth, and release
more of
it on ascent. Thus, if two divers follow identical dive plans, their
computers will indicate the same results--but the diver with more fat
will
be at greater risk for decompression sickness.

Uwatec's manual has a disclaimer for this, too: "each diver will vary
in his
or her susceptibility to decompression sickness. Not only that, but
each

individual diver's own susceptibility may vary from day to day."

These disclaimers need to be taken seriously.

A sufferer from decompression sickness

<http://www.photo.net/travel/diving/decompression-illness>

says he was told that "85% of people treated for decompression illness were diving within limits imposed by tables or a dive computer (i.e., most

people struck by DCI are following the rules)." Dr. Emerson in the article

cited above noted scuba divers can suffer from decompression sickness even

if they religiously follow diving tables.

A sample chapter from a 1997 book by Lawrence Martin, MD,

<http://www.mtsinai.org/pulmonary/books/scuba/sectiong.htm> goes into

considerable detail, but the bottom line is that "For a given individual, [decompression sickness] is unpredictable."

How do divers behave? The article Bell cites about about the allegedly defective computers,

<http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2003/05/25/MN309974.DTL>

says that a pair of divers who "surfaced... then checked their computers

to make sure another dive was safe. 'I look at Mitch's computer and look

at mine,' said Iazdi in his throaty Portuguese accent. 'I say, "We're good."'

Dive computers have the intrinsic RISK of false precision. They do calculations with great precision that simulate sophisticated models and

take care of dozens of details. Unfortunately, the correspondence between

the models and reality is crude.

Even without software flaws, divers are subject to the RISK of believing

something must be true just because it's a "computer" that said so.

Electric utility direct-debit fiasco

Jonathan Kamens <jik@kamens.brookline.ma.us>

Tue, 20 May 2003 20:58:09 -0400

Yet another direct-debit horror story....

Knowing that I was going to be out of town when my next electricity bill came due, and not wishing to worry about having enough money in my checking account to cover it while on vacation, I telephoned my electric company (NSTAR) and asked them to suspend direct debit until further notice.

They agreed, and indeed, the electricity bill which arrived while I was on vacation said "please pay this bill" instead of "your account will be debited on <date>."

Upon my return, I sent the electric company a check and then telephoned them and asked for direct debit to be resumed as of my next bill. I was assured that payment for the bill which arrived while I was on vacation would not be debited from my account.

Two weeks later, when my next bill arrived, I discovered that the payment was, in fact, debited from my account. Thus I had paid twice for the same bill, and NSTAR was holding onto over \$100 of my money to which they were not entitled. As luck would have it, I didn't bounce any checks because of this, but I could have done so easily.

An additional wrinkle is that despite the fact that the total amount due on the new bill was less than the overpayment, the bill still claimed that they would be taking money from my checking account, apparently because when they received my overpayment, they applied all of it as an NSTAR credit and none of it to the supplier half of the bill (I use a third-party electricity supplier).

I contacted the electric company by E-mail and asked them to return the money to me. First, they said that they could only refund the difference between the debit and how much I owed on the new bill, despite the fact that the amount on that bill was not actually due for two more weeks. When I responded that this was unacceptable, they agreed to refund the entire debit amount, but said that it would take two to three weeks for a check to be issued. I said that, too, was unacceptable -- they had no right to that money in the first place, and they should immediately either reverse the debit or issue me a

check and send it via overnight delivery. They refused. I instructed them to immediately and permanently disable direct debit on my account.

I also informed them that I would not be sending any money in response to the new bill, because I had a credit balance greater than the total amount owed, and it was up to them to ensure that the appropriate amount was transferred from that balance to the third-party supplier. They responded that this would happen correctly as a matter of course, i.e., that even though my bill told me to pay the third-party supplier balance, I didn't really need to do so. This is not the first time that the amount due given on my NSTAR bill was different from what they actually debited.

There are many risks here, including:

- * It should be impossible for their billing system to debit an account to satisfy an unpaid balance after sending the customer a bill instructing him to pay the bill manually.

Other utilities in my area get this right. If the bill they send you says "please pay," then you need to pay it, regardless of whether you activate direct debit between when you receive the bill and when it is due.

- * It should be impossible for their billing system to tell the customer that an amount will be debited automatically and then, with no prompting from the customer, debit a different amount or no amount at all.

Putting it another way, the bill that gets sent to the customer should be correct (what a concept!).

- * The billing system should have safeguards in place to automatically detect double payments and bounce them to a human for handling (e.g., contacting the customer and/or sending a refund for the overpayment).
- * They should have procedures in place for reversing unauthorized debits promptly. The only things preventing them from doing this are bureaucracy and an inadequate billing system. It is unreasonable for them to allow these to get in the way of promptly returning money that they stole from customers.
- * The billing system should know how to reconcile credit balances with monies owed to third-party suppliers.

✦ Incremental insecurity (Re: Cohen and Weiss, [RISKS-22.75](#))

Paul Wexelblat <geezer@diapensia.com>

Fri, 30 May 2003 20:04:43 -0400

[RISKS-22.75](#) had a couple of entries that illustrate another RISK:

- * ISP resets password to an easily guessed one (Dawn Cohen)
- * Sensitive data on Web sites reflects lack of security awareness (Rick Weiss)

They point out the insidious problem of secure systems spontaneously becoming insecure through no action of the user. This means that, no matter

how safe and secure any service that has your info may be now, tomorrow they

may change their system or be bought out -- as illustrated in the two cases

above.

What are the chances that either of these outfits will be either willing or

able to remove the compromised data?

...and what are the odds that complaints of violation of privacy statements

will be met with a claim that the "privacy statement" includes a term equivalent to "we reserve the right to make any change we want to to these

terms at any time without notice"?

✦ Re: ATM time sync ([RISKS-22.73](#))

David Leshner <wb8foz@nrk.com>

Tue, 3 Jun 2003 10:01:40 -0400 (EDT)

The arrest of the wrong party based on defective "money machine" timestamps has also occurred in the District of Columbia.

From memory, there was brutal murder and the victim's card had been used after the time of death. The ATM camera's photo got wide play on TV and in the newspapers. The person pictured surrendered with his attorney AND the receipt from his girlfriend's card; he had used it with her permission.

Despite that evidence and an alibi; he was still jailed for about a week before the US Attorney would relent.

I would think there would be the potential for substantial civil litigation against the bank, the ATM network and the machine manufacturer in these cases. Judgments often have the effect of spurring correction of the design errors... (Another RISK, perhaps -- {system} validation by verdict?)

✶ Re: University of Calgary to teach virus writing (Brunnstein, [R-22.75](#))

Nicholas Weaver <nweaver@CS.berkeley.edu>
Fri, 30 May 2003 17:44:47 -0700

I have to strongly second Klaus Brunnstein's comments in comp.risks concerning http://www.cpsc.ucalgary.ca/News/virus_course.html

As a researcher who has analyzed existing worm strategies and developed novel strategies (warhol worms, metasever worms) and plausible defenses, I find the notion of actual virus and worm writing as part of the educational and research process both abhorrent and of effectively NO value.

For evaluating propagation behavior, simulation, "on-paper" evaluations, and analysis of previous worms can tell us effectively all we need to know: How worms and viruses spread, how they interact with many existing and possible defenses, and some requirements (such as automatic reactions) required to build robust defenses.

Simulation predicted the possibility of very fast worms and many of the requirements for automated defenses. Paper analysis insures that I will never run KaZaA myself (the recent vulnerability could be used to take out all supernodes in probably less than <2 minutes). And analysis gives us a treasure-trove of what works well for malicious coders, such as how to cross firewalls and enter local Windows domains.

There are some surprises which come up, such as Slammer/Sapphire's speed, but these are second-order effects. Sapphire was still a scanning worm, so automated defenses which could stop a 1 hour scanning worm should stop a Sapphire-esque worm. Likewise, there are numerous other techniques (Hitlisting & permutation scanning, topological, metaserver) which can create worms that spread to all vulnerable hosts in roughly the same timeframe.

Likewise, to evaluate the defenses themselves, existing attacks can often be used as long as the defense hasn't been pre-trained. For worms which exploit security vulnerabilities, such as Code Red, these are no longer threats, as effectively all vulnerable machines have been patched and effectively all of the remaining machines are infected.

And, if existing attacks, paper design, and simulation are all insufficient to evaluate a defense-mechanism, the best solution is to create daemon programs which run on test machines and who's behavior (eg, system

calls,
network communication) MIMICS the behavior of a worm when
communicating with
other copies of the program, as such program can not spread beyond
the test
machine.

There is room for a good course on malicious code and defenses, but
it need
not, and should not, include construction of self-propagating programs
(worms or viruses).

I do not need to write worms to understand the problem, construct, and
evaluate defenses.

Nicholas C. Weaver
berkeley.edu

nweaver@cs.

✉ Re: University of Calgary to teach virus writing (Brunnstein, [R-22.75](#))

Dan Bornstein <danfuzz@milk.com>
Fri, 30 May 2003 16:37:06 -0700

I'm willing to give the U of C the benefit of the doubt here.

Many years ago I had a lot of fun writing programs for a game called
Core
Wars. The idea of the game (for those unfamiliar with it) was that
your
program and an opponent's program get loaded into a single "core" and
the
goal is for your program to subvert the other one such that the only
threads
of execution left are ones that your program initiated.

This was (a) educational, (b) fun, and (c) arguably a helluva lot like
virus-writing. I don't think writing code for Core Wars games is
immoral,
nor do I think it should be illegal; and I'd be hard pressed to tell
you the
difference between doing that and writing any other code for use in a

controlled, quarantined computing environment, such as is proposed for the course.

[When I was at Bell Labs in the early 1960s, there was a version of core wars that ran on the IBM 70x machines. Doug McIlroy, Vic Vyssotsky, and perhaps Bob Morris will certainly remember that one. PGN]

⚡ Denial of Service via Algorithmic Complexity Attacks

Monty Solomon <monty@roscom.com>

Sat, 31 May 2003 10:22:56 -0400

Denial of Service via Algorithmic Complexity Attacks

Scott A. Crosby <scrosby@cs.rice.edu>

Dan S. Wallach <dwallach@cs.rice.edu>

Department of Computer Science, Rice University

We present a new class of low-bandwidth denial of service attacks that exploit algorithmic deficiencies in many common applications' data structures. Frequently used data structures have ``average-case'' expected running time that's far more efficient than the worst case. For example, both binary trees and hash tables can degenerate to linked lists with carefully chosen input. We show how an attacker can effectively compute such input, and we demonstrate attacks against the hash table implementations in two versions of Perl, the Squid web proxy, and the Bro intrusion detection system. Using bandwidth less than a typical dialup modem, we can bring a dedicated Bro server to its knees; after six minutes of carefully chosen packets, our Bro server was dropping as much as 71% of its traffic and consuming all of its CPU. We show how modern universal hashing techniques can yield performance comparable to commonplace hash functions while being

provably secure against these attacks.

http://www.cs.rice.edu/~scrosby/hash/CrosbyWallach_UsenixSec2003/index.html

http://www.cs.rice.edu/~scrosby/hash/CrosbyWallach_UsenixSec2003.pdf

🔥 REVIEW: "Mission Critical Security Planner", Eric Greenberg

Rob Slade <rlade@sprint.ca>

Tue, 3 Jun 2003 12:00:58 -0800

BKMSCRSP.RVW 20030330

"Mission Critical Security Planner", Eric Greenberg, 2003,
0-471-21165-6, U\$35.00/C\$54.95/UK#25.95

%A Eric Greenberg

%C 5353 Dundas Street West, 4th Floor, Etobicoke, ON M9B 6H8

%D 2003

%G 0-471-21165-6

%I John Wiley & Sons, Inc.

%O U\$35.00/C\$54.95/UK#25.95 416-236-4433 fax: 416-236-4448

%O <http://www.amazon.com/exec/obidos/ASIN/0471211656/robsladesinterne>

<http://www.amazon.co.uk/exec/obidos/ASIN/0471211656/robsladesinte-21>

%O <http://www.amazon.ca/exec/obidos/ASIN/0471211656/robsladesin03-20>

%P 416 p.

%T "Mission Critical Security Planner"

In the introduction, Greenberg claims that his book provides guidance on how to do quantitative security planning without calculations (which sounds somewhat self-contradictory) using a new technique he calls impact analysis (which doesn't sound too different from business impact analysis). A technical background is said to be unnecessary, the process is worksheet based, and the target audience is security managers.

Chapter one says that protecting information is not exact (a statement that doesn't seem to fit well with the worksheet approach). Random security topics include planning, intruders, and a risk analysis example which is, ironically in view of the introduction, more computationally intensive than most. An overview of planning, in chapter two, majors on the minors. Policies are not discussed until

twenty five pages into the material, and then the emphasis is on very specific areas like exit (termination of employment) procedures, leaving huge topics uncovered. Twenty eight security elements are listed, and all are important, but almost all are either over-vague or over-specific.

Chapters three and four introduce the worksheets themselves. Sixteen topic areas have four sheets each, dealing with the technical, lifecycle, business, and "selling to management" aspects of the themes, while other domains may have only a single sheet. The questions listed may be helpful as reminders to address certain aspects which are often overlooked, but the odd and arbitrary structure is confusing, and the real work is definitely left as an exercise to the reader.

A description and analysis of PKI (Public Key Infrastructure), in chapter five, is vague and weak, and contains much unrelated material. Chapter six is a recap of the book, along with a simple list of threats.

While the advice in the book is not wrong or misleading, and many important and useful points are buried throughout, poor organization, a lack of consistent depth, and gaps in topical coverage ensure that the text would only poorly repay the investment of time spent studying it. Certainly it should not be used as a major guide to structure the security planning process.

copyright Robert M. Slade, 2003 BKMSCRSP.RVW 20030330
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca pl@canada.com
<http://victoria.tc.ca/techrev> or <http://sun.soci.niu.edu/~rslade>



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 77

Wednesday 18 June 2003

Contents

- [Cyberterrorists in the U.S. Senate](#)
[Curt Sampson](#)
- [Digital mobile phones can phreak pacemakers](#)
[George Michaelson](#)
- [United Airlines to offer e-mail on domestic flights](#)
[NewsScan](#)
- [\\$24-million spreadsheet "boo-boo"](#)
[Jonathan Levine](#)
- [Crash loses names of Canadian firearms registrants](#)
[Derek K. Miller](#)
- [Scotland Yard outage chaos](#)
[Dave Austin](#)
- [eBay fraud](#)
[John Reinke](#)
- [Tiny tracking chips surface in retail use](#)
[Monty Solomon](#)
- [Smart cellphone would spend your money](#)
[Steve Holzworth](#)
- [Virginia grievance system online - with a slight problem](#)
[Jeremy Epstein](#)

- [Sign someone up to be an organ donor!](#)
[Giles Todd](#)
 - [Continental Airlines check-in computer foul-up](#)
[Steve Bellovin](#)
 - [Downloading data can turn your computer into a server](#)
[griep](#)
 - [Re: U of Calgary to teach virus writing](#)
[Crispin Cowan](#)
 - [Computer bugs and believing reliable sources](#)
[Mark Brader](#)
 - [Re: Slade's Review of Mission Critical Security Planner](#)
[Eric Greenberg](#)
 - [Info on RISKS \(comp.risks\)](#)
-

🔥 Cyberterrorists in the U.S. Senate

Curt Sampson <cjs@cynic.net>

Wed, 18 Jun 2003 14:56:12 +0900 (JST)

The chairman of the Senate Judiciary Committee [Sen. Orrin Hatch, R-Utah]

said Tuesday he favors developing new technology to remotely destroy the

computers of people who illegally download music from the Internet.

http://www.salon.com/tech/wire/2003/06/17/hatch_download/

I don't know that there's much more to be said.

Curt Sampson <cjs@cynic.net> +81 90 7737 2974 <http://www.netbsd.org>

[There's lots more to be said. For example, some software vendors would

like to do that to their competitors, not just to their customers. PGN]

✶ Digital mobile phones can phreak pacemakers

George Michaelson <ggm@apnic.net>

Thu, 12 Jun 2003 10:02:57 +1000

<http://www.newsfactor.com/perl/story/21695.html>

The new generation of digital mobile phones can interfere with many types of heart pacemakers, claims a new study in the Institute of Physics journal Physics in Medicine and Biology. Pacemakers can confuse mobile-phone signals with the heart's own electrical signals, causing a malfunction.

George Michaelson, APNIC, PO Box 2131 Milton QLD 4064, Australia
+61 7 3367 0490 <http://www.apnic.net> ggm@apnic.net

✶ United Airlines to offer e-mail on domestic flights

"NewsScan" <newsscan@newsscan.com>

Wed, 18 Jun 2003 08:35:11 -0700

By the end of the year, United Airlines will become the first domestic airline to offer e-mail on all of its domestic flights. Industry analyst Jonathan Gaw of IDC says the service will be a good attraction for business users, who both need their e-mail and who can expense it." For \$15.98 a flight, a passenger will be able to send and receive e-mail and attachments, by connecting a laptop computer to a jack on the Verizon Airfone

handset

available throughout the plane. [*Baltimore Sun*, 18 Jun 2003;

NewsScan

Daily, 18 June 2003]

[http://www.sunspot.net/technology/bal-bz.
email18jun18,0,7414783.story
?coll=bal-technology-headlines](http://www.sunspot.net/technology/bal-bz.email18jun18,0,7414783.story?coll=bal-technology-headlines)

[And I presume first-class passengers will be offered a plate of Spam as

an appetizer, with Monterey Jack. (And why is Jack always female in this

context?) What about people SENDING spam from the plane?

What about spam

filters for incoming e-mail? Nothing like sitting on a 6-hour flight and

watching your spam pile up. PGN]

✶ \$24-million spreadsheet "boo-boo"

Victor the Cleaner <jonathan@canuck.com>

Wed, 4 Jun 2003 17:08:10 -0600

From *The Calgary Sun*, 4 Jun 2003:

TransAlta Corp said yesterday a "clerical error" was a costly one for the

power producer -- \$24 million US to be exact. The Calgary-based company

said a spreadsheet goof by an employee last April caused the company to

pay higher than intended rates to ship power in New York. CEO Steve

Snyder told a conference call yesterday a "cut-and-paste" foul-up in an

Excel spreadsheet on a bid to New York's power grid operator led TransAlta

to secure 15 times the capacity of power lines at 10 times the

price. The

costly human error couldn't be reversed by the grid operator and while

TransAlta has since tried to recoup the mammoth losses, it was left with a

\$24-million US lesson. [...]

The RISKS? Jeez, where do you start? This sort of thing is becoming so

depressingly common that it barely makes print. Enormously complicated and

powerful tools that are capable of simultaneously magnifying minor errors

and burying from sight the megabuck consequences? The apparent "we're

terribly sorry, but our computers aren't programmed to issue refunds"

response of the "New York power grid operator"?

Jonathan Levine, Middle Digital Inc. <http://www.realweasel.com>

[Also noted by Morty Ovits.

<http://reddeeradvocate.com/editorials/radB948F.htm>

and George N. White III. PGN]

✂ Crash loses names of Canadian firearms registrants

"Derek K. Miller" <dkmiller@pobox.com>

Wed, 04 Jun 2003 15:29:19 -0700

A database crash now threatens to turn people trying to comply with an

unpopular law into lawbreakers instead.

The Canadian government has been attempting to implement a nationwide

firearms registry for several years now. What was originally supposed to

cost at most a few million dollars to document every previously

undocumented
rifle or shotgun in the country has now ballooned into a \$1
billion-plus
megaproject that appears not to work.

http://www.cbc.ca/news/features/firearms_act.html

Even those, like me, who are firmly for Canada's strong gun-
control laws
find the way this project has been put together to be laughable
(and that's
a charitable assessment). In many rural parts of Canada, a long
gun is a
necessity, at least to hunt for food or as protection against
potentially
dangerous wildlife (everything from polar bears to moose and
wolverines,
depending on where you are) for people living or working in the
bush, from
native communities to petroleum exploration teams.

The latest registry mishap to come to light is that the database
software,
overloaded before the registration deadline was extended several
months from
its original 1 January 2003 date, crashed, and apparently took
some
registrants' names with it. No one seems to know how many, and I
haven't
been able to track down any details of the kinds of software or
platforms
that were in use.

[http://www.ctv.ca/servlet/ArticleNews/story/
CTVNews/1054726691584_31/](http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/1054726691584_31/)

To add to the federal government's trouble, a number of
provinces have now
said they will refuse to prosecute people who flout the act by
not
registering their guns -- and there are many such scofflaws.

>From the CTV article above:

> The federal Firearms Act and the Criminal Code state that anyone possessing a
> firearm as defined in Section 2 of the Code must hold a valid firearms
> registration certificate. The new legislation requires that owners of
> long-guns such as rifles and shotguns, register their weapons by July 1 or
> face legal action.
>
> Critics of the gun registry have argued that the legislation is nothing more
> than a costly waste of time.
>
> The auditor general has projected it could end up costing more than \$1
> billion by 2005 rather than the net \$2 million over 10 years projected
> when it was established in 1995. And many say people who would use their
> firearms for violent offences aren't likely to register their guns anyway.

Aside from the direct risks of setting up a database without the bandwidth
or computational headroom for large increases of traffic before a deadline,
lacking proper file journaling, and insufficiently backed up, there is the
additional risk that the predictable failure of such a system will cast
further bad light on a project already suffering from a reputation for
inefficiency and poor planning.

Derek K. Miller - dkmiller@pobox.com
[Also noted by Dan Haggarty. PGN]

Scotland Yard outage chaos

"Dave Austin" <dave.austin@insight.co.uk>

Fri, 6 Jun 2003 11:01:37 +0100

I thought that this was of interest, an old risk but surprising to find such a high profile building vulnerable:

Yard crisis as power fails , 4 Jun 2003

Scotland Yard was plunged into crisis today by a massive power and communications failure. All phones in the building were cut off as all lines to the Yard were down, while the central system for handling 999 calls also failed and had to be switched to local police stations. Computers which log emergency and other calls to police in London - known as the CAD system - failed, along with a second system to Hendon which was supposed to provide an emergency back-up. Emergency generators restored power to the building, but officers had to resort to using mobile phones. A group of senior officers was called together to handle the crisis. One police source said the meeting had examined the possibility that the power failure was a terrorist or a criminal act, though this had been ruled out. The failure showed the vulnerability of the Yard's communications network at a time when London is on alert for a possible terrorist outrage. The phones and electricity crashed at about 9.30am and were still out of action two hours later. A Yard spokesman said the crisis was caused by a single workman cutting through an electricity cable in the Victoria area, and that the company's chief executive had personally apologised to senior

officers. As engineers from the Yard and outside companies were working flat-out to solve the problem, the police spokesman emphasised that officers were still responding to 999 calls which had been routed through the main London police stations. "We have contingency plans in place which are working well," added the spokesman. "We are still able to provide emergency cover for London. "This is a serious matter and we are seeking to bring the building back on-line as quickly as possible." One employee at the building said: "We're in the hands of the engineers." Asked if it was causing huge problems, he said: "You could say that." Visitors to the Yard's reception who had fixed appointments were told they couldn't be seen today because of "internal communication problems". Staff at reception were unable to make internal phone calls and unless visitors had the mobile phone numbers of staff they were due to meet, they were told they would not be able to see them. Other buildings in the area were also affected by the blackout. London Ambulance said its 999 service was still operational but calls were being handled on paper for about an hour and a half while the power was disrupted. Scotland Yard has contingency plans to relocate its emergency systems and senior officers in the event of a massive crisis such as a terrorist attack. However, this did not happen this morning. Another police source said: "This could come from the plot of a film. "One wonders whether there is a massive criminal heist going on somewhere in London.

"The fact that someone can bring the building to a halt by cutting a single cable is a little alarming. "I am sure there will be a few internal inquiries about this."

Police chiefs told to explain blackout

5 June 2003

Police chiefs have been ordered to provide a full report into the power failure which led to computers and telephones at Scotland Yard crashing for more than seven hours. Toby Harris, chair of the Metropolitan Police Authority, said there were "grave concerns" after an engineer blacked out the HQ yesterday by accidentally cutting a single cable in the street. He added it called into question the Met's ability to cope in a crisis.

Source: (London) Evening Standard - also covered in The Times et al.

Dave Austin <dave.austin@insight.co.uk> www.insight.co.uk

eBay fraud

"John Reinke" <reinke@att.net>
Fri, 13 Jun 2003 09:14:12 -0400

Police in South Salt Lake, Utah, are working with eBay to determine just how many people were victimized by what authorities say was one of the biggest frauds in the auction site's history. Police arrested 31-year-old Russell

Dana Smith last weekend after hundreds of auction winners complained that they sent \$1,000 or more to a company named Liquidation Universe for laptop computers they never received. Police say the firm appears to have raked in \$1 million from about 1,000 victims in just a few weeks. [...]
[Source: Bob Sullivan, MSNBC, Man arrested in huge eBay fraud; Buyers criticize auction site's seller verification service]
<http://www.msnbc.com/news/925433.asp?0dm=C12LT>

[FJR: Guarantees are only as good as the guarantor. There ain't no free lunch. When will people take security seriously?]
[This one is a long and ugly story. PGN]

🔥 Tiny tracking chips surface in retail use

Monty Solomon <monty@roscom.com>
Tue, 10 Jun 2003 01:34:38 -0400

Tom Pounds waved his overflowing grocery basket at the wall and offered a glimpse of our shopping future. The coffee cans, razor blades, and other items in his basket each carried a stowaway -- a tiny chip, the size of a fleck of black pepper, coupled with an antenna. Each emitted a short burst of identifying data that streamed via radio waves to a sensor on the wall. [...]
Within fractions of a second, a computer translated those received signals onto a monitor as images of each product in the basket. [...]
In 15 or 20 years, futurists predict, the pervasive RFID tags will

link to
massive computer networks, enabling speedy checkout from the
grocery store,
medicine cabinets that tell you when to take pills, and milk
cartons that
inform your fridge when to add another gallon to the grocery
list. [...]
[Source: Chris Gaither, Radio Frequency Identification Tiny
tracking chips
surface in retail use Retail uses for ID chips surfacing, *The
Boston
Globe*, 9 Jun 2003]

[http://www.boston.com/dailyglobe2/160/business/
Tiny_tracking_chips_surface_in_retail_use+.shtml](http://www.boston.com/dailyglobe2/160/business/Tiny_tracking_chips_surface_in_retail_use+.shtml)
[Tiny_tracking_chips_surface_in_retail_use+.shtml](http://www.boston.com/dailyglobe2/160/business/Tiny_tracking_chips_surface_in_retail_use+.shtml)

Smart cellphone would spend your money

Steve Holzworth <sch@unx.sas.com>
Tue, 17 Jun 2003 11:32:52 -0400

"A consortium of the world's top consumer electronics firms,
mobile
networks and broadcasters are funding the development of
cellphones that
will spend money on your behalf. The consortium, called Mobile
VCE,
includes Nokia, Sony, Vodafone and the BBC. It might sound
like a
bankruptcy waiting to happen, but software engineer Nick
Jennings is
supremely confident the phones will not mess up anybody's
life. [...]
The cellphone agents only offer help if triggered by a diary
event or if a
definite pattern of behaviour, such as going to the movies
every Friday,
has been established." [Source: New Scientist]

<http://www.newscientist.com/news/news.jsp?id=ns99993818>

[SCH - how many "supremely confident" software engineers have watched as their rocket booster exploded, their online store got hacked, etc.?)

What mechanisms will be in place to dispute or refuse purchases that your cellphone agent makes on your behalf? Be **sure** that you always want to go to the movies every Friday...

I own a DirecTivo video recorder, which has a similar agent-like process that automatically records "suggested" programs for you, based on analyzing your previous viewing habits. I'm still often amused by some of the "suggestions" it makes, which have no obvious relevance whatsoever to my typical viewing habits.

I suppose that if your life runs on a rigid schedule, this might be useful. My life certainly doesn't...

Steve Holzworth Senior Systems Developer SAS Institute - Open Systems R&D
VMS/MAC/UNIX, Cary, N.C. sch@unx.sas.com

⚡ Virginia grievance system online - with a slight problem

Jeremy Epstein <jeremy.epstein@webmethods.com>
Fri, 6 Jun 2003 11:10:44 -0400

Virginia put its workplace grievance system online as a way of improving

responsiveness (the old system typically took a year to process), according to *The Washington Post* Expected savings are \$100,000/year, possibly more.

As a Virginia taxpayer, that's good.... every little bit helps.

[<http://www.washingtonpost.com/wp-dyn/articles/A10481-2003Jun3.html>]

"The system is secure from prying eyes, yet those who need to know a case history can view an entire file by using the employee's Social Security number." So... yet another new system that uses the employee's SSN as the key. That's bad. [And we won't even get into how they know that "the system is secure from prying eyes".]

✂ Sign someone up to be an organ donor!

Giles Todd <g@todd.nu>

Fri, 13 Jun 2003 22:22:23 +0200

Add anyone you like to the UK's NHS Organ Donor Register at:

<https://www.uktransplant.org.uk/odronline/servlet/mydetailsservlet>

Apart from trivial address validity checks, the sole attempt to ensure that

the person being signed up is really who he or she says he or she is is an

e-mail message sent to the e-mail address supplied.

Date: Fri, 13 Jun 2003 21:11:12 +0100 (BST)

From: odr@uktransplant.nhs.uk

Subject: I want to be a donor

Thank you for joining the NHS Organ Donor Register. Your new

record will
now be downloaded directly to the register.

If you wish to amend the personal information held on the register at any time you can do so through this website, or by contacting:
The Organ Donor Line (0845 60 60 400) between 7am and 11pm seven days a week for a form, or by writing to:
The NHS Organ Donor Register, UK Transplant, PO Box 14, FREEPOST
Patchway, BRISTOL BS34 8ZZ UK

✶ Continental Airlines check-in computer foul-up

Steve Bellovin <smb@research.att.com>
Sat, 14 Jun 2003 13:35:54 -0400

This morning, I tried to check in for a Continental flight from Newark to Seattle. But all of the self-service check-in kiosks and all of the domestic check-in computers were down. It seems that they'd done a software upgrade at 0200, and when things got busy the system died. One of the customer service managers was muttering that they should have installed the upgrade on a Sunday morning instead.

They told people to go upstairs to the International check-in area, which hadn't been "upgraded". But they didn't allocate enough desks -- or enough people from the non-functional domestic check-in -- to handle the crowd. Nor, despite assurances from Customer Service, did they hold any flights. The system wouldn't let me check in 10 minutes prior to flight

time, of course, which is reasonable under normal circumstances but not when their own software has fouled things up. They also didn't have any priority procedure for folks on earlier flights.

But it turns out that they did hold the flight, or so it seems -- checking the Continental Web site when I got home, I found that my flight took off 25 minutes late.

In possibly-unrelated computer confusion, one of the arrival status monitors at EWR was displaying the Internet Explorer "this page is not available" screen, while one of the departure monitors was showing a typical Windows desktop. Hmm -- looking at the pictures I took, I see that it has Winzip installed....

Steve Bellovin, <http://www.research.att.com/~smb>

✶ Downloading data can turn your computer into a server

grep <grep@mindspring.com>
Fri, 6 Jun 2003 12:49:02 -0700

The Register reports (<http://www.theregister.co.uk/content/6/31080.html>) that Joltid is using "content distribution technology that utilises users' own PCs to disseminate content for publishers." According to the article, when someone loads content (such as software) using the Joltid

system, the computer loading the data then becomes a server for that same data.

There seem to be a number of potential risks to users of such a system:

They could held liable for "publishing" information over which they have no control. This liability could include copyright and patent infringement.

If the content is found to contain viruses or material which is illegal, the liability could be even more severe.

Bugs in the Joltid software could expose their personal files to the outside world, even if their computers run no other server software.

Their own network throughput, or other computer resources, might be affected by having their computers act as servers.

They may be subject to additional ISP charges for excessive outbound traffic.

People who retrieve data from another customer's computer (not from the original publisher) need to consider the possibility that the data has been altered. The article does say: "All files are digitally signed to prevent tampering, the company claims", but no details are provided.

⚡ Re: U of Calgary to teach virus writing (Weaver, [RISKS-22.76](#))

Crispin Cowan <crispin@immunix.com>

Sat, 14 Jun 2003 14:53:10 -0700

How is it that worms specifically, or malicious code in general, is a legitimate area of research, but not a legitimate study topic for students in a class? How are we to obtain more defensive experts such as Weaver if we do not train young people in the area.

Techniques to write viruses and worms are evidently already very well known in the black hat community, as evidenced by the proliferation of such worms. It is only in the defensive community where ignorance is relatively common, as evidenced by the naive defenses that are proposed over and over again. In light of that, how is the suppression of malicious coding techniques in the education system any different from the suppression of how to sharpen a pointed stick with which to murder one's neighbor?

I'm sorry, but the cat is clearly out of the bag, and there is little benefit in attempting to suppress knowledge of how to write a worm. IMHO, all the hand-wringing over this course is badly misplaced.

Crispin Cowan, Ph.D. <http://immunix.com/~crispin/>
Chief Scientist, Immunix <http://immunix.com>
<http://www.immunix.com/shop/>

Computer bugs and believing reliable sources

Mark Brader <msb@vex.net>
Fri, 13 Jun 2003 17:13:52 -0400 (EDT)

Back in comp.[risks 22.73](#), Monty Solomon quoted

<<http://finance.lycos.com/home/news/story.asp?story=34131541>>:

| Computer bugs have been around since malfunctions in a 1945
| [Harvard] Mark II were blamed (facetiously) on a moth trapped
| in a relay.

In fact, the malfunction in question *was* caused by the moth trapped in a relay -- the facetious part was the association of this event with the existing slang term for a problem, i.e. "bug". As <http://americanhistory.si.edu/csr/comphist/objects/bug.htm> shows, the moth was preserved along with the annotation, "First actual case of bug being found". (Note the word "actual".)

Now that's not Risks-worthy, but I think the other error in the quoted sentence is: the Lycos writer gave the date of the incident as 1945. As the web page I just cited shows, the logbook with the moth now belongs to the Smithsonian Institution's National Museum of American History, and *they* say that the correct date is 1947. Since the illustrated page does not show the year, I e-mailed info@si.edu to query the point. They replied to say that 1947 is correct and that "The year does not appear on the page, but it does appear elsewhere in the logbook."

Now try a google search for the phrase "first computer bug" and each of the years 1945 and 1947. Go ahead, I'll wait... But here are the counts I get when I do it.

"first computer bug" 1945	388
"first computer bug" 1947	140

Of course, some of these will be false hits -- the year being

mentioned in
another context on the same web page -- but it's easy to see
from the google
synopses that many of the 388 hits do give the wrong date.
Among these are:

<http://www.history.navy.mil/photos/images/h96000/h96566kc.htm>

<http://www.computer.org/history/development/1945.htm>

and a *large* number of university sites. Obviously sources
that you would
expect things to be right, aren't they? I even found one page
(but I lost
it again, so no cite) that seems to show Grace Murray Hopper,
who was part
of the group working on the computer, herself saying that the
incident was
in 1945.

And it's actually even worse than the above numbers suggest. Of
the 140
hits in the second (1947) search, many *are* false. If you
search for the
phrase together with *both* years, there are 103 hits, and many
of these are
pages that date the incident to 1945 and then mention 1947 in
another
context.

Everyone learns quickly enough that you can't believe everything
you
read on the Web. But in this case there are enough pages at
enough
reliable-seeming sites that it's hard to believe that they're all
wrong -- and yet (unless my correspondent at the Smithsonian,
where
the actual logbook is, was lying or mistaken) they are.

The difference between a 1945 and 1947 date for a minor piece of
etymological history is a trivial error to practically
everyone. But the
next time you believe what you read, it might not be trivial.

(Of course this sort of problem can happen with non-Internet research too. The Risks relevance is that Web searching makes it so much easier to become very sure very fast...)

Mark Brader | "I'm a little worried about the bug-eater",
she said.
Toronto | "We're embedded in bugs, have you noticed?"
msb@vex.net | -- Niven, "The Integral
Trees"

✶ Re: Slade's Review of Mission Critical Security Planner

"Eric Greenberg" <eric@netframeworks.com>
Mon, 16 Jun 2003 09:14:49 -0400

My book titled Mission Critical Security Planner (Wiley, 2003), which Slade has critiqued here, survived full scrutiny and review on slashdot.org, a tough group of folks

<http://books.slashdot.org/article.pl?sid=03/02/13/1515257>

and has been reviewed by many reviewers, all of which have offered nothing but praise. I encourage you to see the other reviews on Amazon.com and elsewhere on the Internet.

<http://www.amazon.com/exec/obidos/ASIN/0471211656>

You might also visit the Mission Critical Security Planner companion Web site, where you can download a free electronic copy of the Chapter 1 and the free worksheets used in the book, at

<http://www.CriticalSecurity.com>

Judge my commitment to this book, supporting the readers, and security planning in general, by that material and the Web site.

Eric Greenberg <http://www.CriticalSecurity.com>
<http://www.amazon.com/exec/obidos/ASIN/0471211656>



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

[ACM](#) Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 78

Saturday 28 June 2003

Contents

- [Cancer therapy missed tumor sites](#)
[John Colville](#)
- [Fear of flying? You just might be a terrorist!](#)
[Dawn Cohen](#)
- [How Hulk Crushed the Online Pirate](#)
[P.J. Huffstutter via Monty Solomon](#)
- [E-Mail Swindle Uses False Report About a Swindle](#)
[Hafner-Flynn via Monty](#)
- [New bill injects FBI into P2P battle](#)
[David Becker via Monty Solomon](#)
- [RFID Chips Are Here](#)
[Scott Granneman via Monty Solomon](#)
- [Cell-phone tracking](#)
[David Leshner](#)
- [Student arrested for allegedly derailing election](#)
[John Reinke](#)
- [ISP's DHCP servers infiltrated](#)
[Tom Van Vleck](#)
- [Wireless gives poorer nations chance to catch up ...](#)
[NewsScan](#)

- [Big sites hoard links](#)
[Monty Solomon](#)
 - [Crossing Dateline a navigational risk](#)
[John Elsbury](#)
 - [More erroneous arrests over erroneous ATM clocks](#)
[David Leshner](#)
 - [Re: Soyuz landing problem caused by software?](#)
[Peter B. Ladkin](#)
 - [Virgin Mobile makes the oldest mistake in the book](#)
[Jay R. Ashworth](#)
 - [PayPal fraud, and the importance of grammar](#)
[Geoffrey Brent](#)
 - [When spam filters go bad](#)
[Laura Miller via Monty Solomon](#)
 - [New State Laws on Privacy](#)
[Robert Ellis Smith](#)
 - [Monty Solomon <monty@roscom.com>](#)
 - [Secure Coding Principles and Practices, Graff/van Wyk](#)
[Monty Solomon](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ Cancer therapy missed tumor sites

<colville@it.uts.edu.au>

Mon, 23 Jun 2003 11:55:00 +1000

Ten critically ill patients with advanced lung or esophagus cancer were given radiation therapy to the wrong spot in the past four years, doctors from Prince of Wales Hospital admitted. Eight of those patients (who were all at the end stages of their illness) have died, although none of them reportedly died as a result of the mistake. The rare treatment (1% of the therapy cases) delivers radiation via a

flexible catheter to the tumor site and was reportedly off by millimeters -- although centimeter adjustments may be expected to compensate for breathing variances. Two other patients had the same incorrect treatment in 1993 and 1995. (This treatment is apparently used only for incurable cases, to relieve symptoms.) An investigation is under way to determine the extent of the error, which occurred when the wrong details were entered into a computer used to control the delivery of the therapy. [Source: Ruth Pollard, *Sydney Morning Herald*, 21 Jun 2003; PGN-ed, with American spelling]

<http://smh.com.au/text/articles/2003/06/20/1055828490830.htm>

John Colville, Department of Computer Systems, University of Technology, Sydney
PO Box 123, Broadway NSW Australia 2007 +61-2-9514-1854
colville@it.uts.edu.au

✶ Fear of flying? You just might be a terrorist!

"Dawn Cohen" <COHEND@wyeth.com>
Mon, 23 Jun 2003 15:06:00 -0400

It was reported this morning on Public Radio International's Marketplace program that a company called QinetiQ is trying to market an "intelligent" airplane seat that would detect nervousness in passengers and alert airline staff. Essentially, it sounded like a motion detector and profiler.

QinetiQ appears to be a spin-off for Britain's Defense Evaluation Research Agency (sounded like the British DARPA or some kind of government lab, from the story.)

I found it interesting that the first half of the story focused on the terrorism potential for this technology, but the rest of the story went on to outline how helpful it could be for personalizing your flying experience. From the report, it sounded like if you squirmed around a lot or shook for some reason, you might be brought to the attention of the crew, as a potential terrorist. Of course, there would be health benefits, as well: if you sat still for too long the crew could warn you to move around a little to avoid blood clots in your legs. And by the way, the intelligent seat would have some kind of card reader that would let the passenger swipe their personal card to pick a movie to see or to specify other flight options.

I'm not sure if this is a marketing ploy wrapped as an anti-terrorism product or an anti-terrorism ploy wrapped as a marketing product. Either way, it seems like it has good potential for mis-use.

I wonder how many false positives it will take to have the staff turn the system off altogether. I imagine it would be kind of irritating to the crew to have to investigate squirming 2 year olds, people with ADD, people who have various anxiety conditions, people flying to high stakes business presentations, oh yeah, and people who look like they might be from the Middle East, who might just be a little nervous because they've been profiled before.

✶ How Hulk Crushed the Online Pirate

Monty Solomon <monty@roscom.com>

Thu, 26 Jun 2003 23:57:05 -0400

On 25 Jun 2003, Kerry Gonzalez, a 24-year-old New Jersey insurance underwriter, pleaded guilty in a Manhattan federal court to criminal charges of posting a bootlegged early non-final copy of the new movie "The Hulk" on the Internet. He could face a maximum sentence of three years in prison and a fine of \$250,000 when he is sentenced Sept. 26 in U.S. District Court for the Southern District of New York. [Source: P.J. Huffstutter, *Los Angeles Times*, 26 Jun 2003] <http://www.latimes.com/business/la-fi-hulk26jun26224419,1,1391001.story>

✶ E-Mail Swindle Uses False Report About a Swindle

Monty Solomon <monty@roscom.com>

Sat, 21 Jun 2003 22:12:36 -0400

By KATIE HAFNER and LAURIE J. FLYNN, *The New York Times*, 21 Jun 2003

SAN FRANCISCO, June 20 - It was a clever, if not entirely flawless ruse. Many of its potential victims saw through it immediately. Others were less skeptical and were caught in its snare.

On Wednesday, starting in the early afternoon, people around the country began receiving an e-mail message with "Fraud Alert" in the

subject line. In the guise of concern about a purchase from Best Buy and possible credit card misuse, the message urged recipients to go to a "special" BestBuy.com Web site and correct the problem by entering their credit card and Social Security numbers.

E-mail posing as a fraud notice to carry out a fraud - indeed preying on a consumer's fear of being defrauded - is an illegal form of spam, the much-loathed tide of random, unsolicited messages that pours into computer inboxes every day. ...

<http://www.nytimes.com/2003/06/21/technology/21CARD.html>

🔥 New bill injects FBI into P2P battle

Monty Solomon <monty@roscom.com>
Sat, 21 Jun 2003 23:45:18 -0400

David Becker, CNET News.com, 20 Jun 2003

A bill introduced in Congress on Thursday would put federal agents in the business of investigating and prosecuting copyright violations, including online swapping of copyrighted works. HR-2517, the Piracy Deterrence and Education Act of 2003, instructs the FBI to develop a program to deter online traffic of copyrighted material. The bureau would also develop a warning, with the FBI seal, that copyright holders could issue to suspected violators. And the bureau would encourage sharing of information on suspected copyright violations

among law enforcement, copyright owners and ISPs (Internet service providers).

The bill bears the names of two legislators who have been prominent on intellectual property and copyright issues--Reps. Lamar Smith, R-Texas, and Howard Berman, D-Calif. Berman gained attention last year with a bill that would have allowed copyright holders to hack into peer-to-peer networks believed to be distributing protected materials.

The new bill also calls for the Department of Justice to hire agents trained to deal with computer hacking and intellectual-property issues, and it requires the Attorney General, in conjunction with the departments of Education and Commerce, to develop programs to educate the public on copyright issues.

A lawyer with the Electronic Frontier Foundation said the bill includes a number of troubling aspects, particularly the blurring of distinctions between official prosecution of criminal acts and civil enforcement of copyright provisions. ...

<http://news.com.com/2100-1028-1019811.html>

RFID Chips Are Here

"monty solomon" <monty@roscom.com>

Fri, 27 Jun 2003 17:49:36 -0400

RFID chips are being embedded in everything from jeans to paper money, and your privacy is at stake. [Scott Granneman, Security Focus, 26

Jun 2003]

<http://www.securityfocus.com/columnists/169>

✶ Cell-phone tracking

David Leshar <wb8foz@nrk.com>

Sun, 22 Jun 2003 12:05:26 -0400 (EDT)

IRS Headquarters employee LaToya Taylor vanished after meeting her ex-BF for lunch. Police searching in Southern MD, an hour+ away from DC recovered a body that may be hers. Why look there?

<<http://www.washingtonpost.com/wp-dyn/articles/A14423-2003Jun19.html>>

The search in Southern Maryland came after police reviewed the records of Taylor's cell phone. They determined that at least

one call was made to her cell phone last weekend while it was in the

Newburg area; the call was unanswered.

This speaks to a level of log retention by cell carriers that has not

been admitted to before. The FCC is requiring [[RISKS-22.69](#)]

"enhanced

911" but in reality such location-tracking can function whenever the

phone is powered-up. One wonders how long before divorce attorneys

start subpoenaing same, and employers demand access as a condition of

employment.

✶ Student arrested for allegedly derailing election

"John Reinke" <reinke@att.net>

Tue, 24 Jun 2003 12:14:39 -0400

Student arrested for allegedly hacking university computers to
derail
election

Shawn Nematbakhsh, a 21-year-old student at the University of
California at Riverside, was arrested for allegedly hacking into
a
university computer system during student elections and casting
800
votes for his own fabricated candidate (American Ninja). (He
told
police he was trying to point out that the UCR network was
vulnerable.)

The election will be redone next month. [Source: Associated
Press, 21

Jun 2003; PGN-ed]

<http://famulus.msnbc.com/famulusgen/ap06-21-053420.asp?t=APNEW>

Good thing it was a made up candidate. Otherwise they might not
even
have known! Computer security is an "art" just like brain
surgery.

But, "anybody" can do it. I just read this and chuckle. Can
government do any thing "right". And, some want to run real
elections
this way? John

F. John Reinke, 3 Tyne Court, Kendall Park, NJ 08824
732-821-5850 reinkefj@yahoo.com

ISP's DHCP servers infiltrated

Tom Van Vleck <thvv@multicians.org>

Fri, 20 Jun 2003 15:33:15 -0400

<http://ask.slashdot.org/article.pl?sid=03/06/19/2325235&mode=thread&tid=126&tid=172&tid=95>

"... It turns out, Charter Communications' DHCP servers were infiltrated and were providing p5115.tdko.com as the 'Connection-specific DNS suffix', causing all non-hardened Windows (whatever that means in a Windows context) machines to get lookups from a hijacked subdomain DNS server which simply responded to every query with a set of 3 addresses (66.220.17.45, 66.220.17.46, 66.220.17.47).

On these IPs were some phantom services. There were proxying Web servers (presumably collecting cookies and username/password combos), as well as an ssh server where the perpetrators were most likely hoping people would simply say 'yes' to the key differences and enter in their username/password..."

Hmm, my cable ISP was down this morning. Maybe coincidence.

⚡ Wireless gives poorer nations chance to catch up ...

"NewsScan" <newsscan@newsscan.com>

Fri, 27 Jun 2003 08:36:17 -0700

In a speech prepared for a UN conference on the social implications of wireless communications technologies, UN Secretary-General Kofi Annan declared that wireless Internet access has "a key role to play everywhere, but especially in developing countries and countries with economies in

transition... It is precisely in places where no infrastructure exists that Wi-Fi can be particularly effective, helping countries to leapfrog generations of telecommunications technology and infrastructure and empower their people." (Reuters, 26 Jun 2003)
<http://asia.reuters.com/newsArticle.jhtml?type=internetNews&storyID=2998152>

... But needs to be watched for security breaches

Using a laptop with a wireless card outside the main office of a Palo Alto, California school district, a reporter was able to gain access to such data as grades, home phone numbers and addresses, emergency medical information, student photos, and psychological evaluations. Unlike the majority of the district's information, the documents available on this wireless network were not password-protected. Superintendent Mary Frances Callan says: "I don't see this as such a huge news story." The real story, says Callan, is the great progress represented by the network itself, which was made possible by new software purchases, employee training sessions, and technology-use policies. (*Palo Alto Weekly*, 25 Jun 2003)
http://www.paloaltoonline.com/paw/paonline/weekly/morgue/2003/2003_06_25.wire25.html

NewsScan Daily, 27 Jun 2003

⚡ Big sites hoard links

Monty Solomon <monty@roscom.com>

Mon, 23 Jun 2003 01:52:25 -0400

**Technology Research News*, 23 Jun 2003*

The Internet is scale-free, meaning it is made up of a few nodes, or servers, that have many links, and many nodes with only a few links.

It is also a small-world network -- you can get to any node via only a few links among adjoining nodes.

University of London researchers have uncovered another clue about the Internet's structure-the rich-club phenomenon. Large, well-connected nodes have more links to each other than to smaller nodes, and smaller nodes have more links to the larger nodes than to each other. ...

http://www.technologyreview.com/articles/rnb_062303.asp

✈ Crossing Dateline a navigational risk

John Elsbury <john.elsbury@sovereign.co.nz>

Mon, 23 Jun 2003 12:26:42 +1200

- > Late last week a twin-engined aircraft on a delivery flight from Samoa to
- > New Zealand - a course a few degrees west of south - missed NZ due to a
- > navigational error and had to be rescued after they set off their ELB.
- > They had ended up a long way to the east of New Zealand and, fortunately,
- > had enough fuel to get to an airport once they had been

located by a
> samaritan flight.
>
> The reported cause was "When they crossed the Date Line, they
should have
> reconfigured the navigation computer for Western Hemisphere
coordinates
> but did not do so". It seems, then, that on crossing the
date line (a
> fair distance north of NZ) they started heading as many
degrees east of
> south as they had hitherto been flying west of south - at
least, it looks
> that way on the map.
>
> They were in bad weather, so I can understand not noticing a
fairly sudden
> change in the relative locations of the moon and stars - but
that, surely,
> ought to have shown up on the magnetic compass?
>
> Regards
> John Elsbury

⚡ More erroneous arrests over erroneous ATM clocks ([RISKS-22.76](#))

David Lesher <wb8foz@nrk.com>
Sun, 22 Jun 2003 11:29:52 -0400 (EDT)

<http://www.washingtonpost.com/wp-dyn/articles/A19633-2003Jun21.html?nav=hptop_tb>

By Ruben Castaneda, *The Washington Post*, 22 Jun 2003; Page A01

For nearly a year after Denise Mansfield was strangled in her
Prince

George's County home last June, police focused their investigation on three female suspects whose identities were a mystery. A surveillance camera videotaped them getting cash from an automated teller machine where Mansfield's missing debit card was used after her slaying. The time of the withdrawal from the dead woman's account, recorded by a bank computer, corresponded to the times stamped on the ATM video of the suspects. ... A SunTrust Bank spokesman declined to comment on the time discrepancy. But Fredrik Nilsson, director of business development for Axis Cameras, which provides video surveillance systems to business and government agencies, said most bank cameras are not synchronized with ATM transactions. The times are set separately and can be off by a few minutes, or even an hour if someone forgets to reset them for daylight saving time, Nilsson said.

{and ANOTHER group of victims...but low-tech}

The arrests of the three Arizona residents were not the only ones to result from the wrong ATM pictures. Last winter, police charged a pair of sisters from the District with murdering Mansfield after a third sister misidentified them in the surveillance images, which were published in The Post and shown on local TV newscasts. The two were jailed for several weeks, until DNA tests exonerated one of them and the other proved that she had been away on a business trip when the killing occurred.

- - - - -

This was not the District ([RISKS-22.76](#)), rather adjacent Prince

Georges County, but the behaviour of the authorities seems virtually identical. [PG is ...noted.. for officer shootings of suspects and unwitnessed confessions, later found untenable. There were allegedly going to be locked cameras installed in the interrogation rooms but I see no mention of same.]

In both cases, there was available evidence that the accused had a legitimate reason to be at the ATM. Yet the bank/police did not even LOOK at adjacent transactions in the ATM log? (That would have ID'ed the AZ women immediately.) This after the publicity over the DC mis-identification???

The RISK here is not just faulty timestamps, but faulty analysis of them, and lack of critical thinking by supposedly-expert investigators, and the prosecutors on the case.

When dangled a "high-tech" bone, Officer McGruff grabbed the bone and ran, without worrying about other details. Given the growing number of cameras recording our every move, the concept that mere presence near the time of a crime is sufficient to establish guilt unless proven innocent, is downright scary.

[Re: Soyuz landing problem caused by software? \(Bellovin, Risks 22.74\)](#)

"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>
Wed, 25 Jun 2003 10:35:56 +0200

In [RISKS-22.74](#), Steve Bellovin summarised an article by James Oberg on the Soyuz TMA-1 ballistic reentry on 4 May, 2003. The Oberg article also raised questions of human error.

According to the article "Soyuz probe reveals human errors" by Tim Furniss in Flight International, 17-23 June, 2003, p39, the ballistic reentry was caused by a failure in the Busp-M guidance system that controls the normal reentry. Busp-M reads data from gyroscopes and accelerometers and outputs commands to the attitude control system. The yaw control channel "produced undefined readings indicating a malfunction", which resulted in Busp being taken off-line by supervisory control, which switched to ballistic reentry. Busp had performed 49 "flawless" reentries since 1979. The article does not say what caused the "undefined readings".

The human errors were unrelated. The crew switched on the Kurs rendezvous-docking system by mistake during reentry; failed to inform search aircraft that they were performing a ballistic reentry; and made mistakes in landing procedures.

An earlier *Flight International* article, 3-9 June 2003, p26, reported the change to ballistic reentry as having been caused by a "faulty gyroscope switch".

Peter B. Ladkin, University of Bielefeld, Germany
<http://www.rvs.uni-bielefeld.de>

✶ Virgin Mobile makes the oldest mistake in the book

"Jay R. Ashworth" <jra@baylink.com>

Thu, 19 Jun 2003 20:12:37 -0400

My sister got a new cellphone the other day. From Virgin Mobile, though they're reselling SprintPCS's airtime.

The e-mail that she got read like this:

```
- ----- Forwarded message follows -----  
Date sent: Thu, 19 Jun 2003 04:19:29 -0700 (PDT)  
From:      ourteam@virginmobileusa.com  
To:       nobody@example.com  
Subject:   Virgin Mobile - Your Cell Number and phone  
programming instructions
```

Hi CINDY,

Ready for this?

Your Virgin Mobile Phone Number: (727) 123-4567
Your Virgin Mobile Phone's Network ID: 007271234567

(Give your friends your phone number, but keep the super secret Network ID to yourself, you might need it to program your phone... this message may self-destruct.)

[lots of administrivia elided]

Welcome to Virgin Mobile - It doesn't get any easier than this!

Enjoy!

Virgin Mobile USA

If you need to contact us, please call Central Intelligence on (888) 322-1122 or *VM from your Virgin Mobile cell phone,

alternatively visit us
at www.virginmobileusa.com

- ----- End of forwarded message -----

So, did everyone notice the format and contents of that "super secret Network ID"? I've modified it, of course, for this message, but yes, they're the same. Central *Intelligence*? Guess it's just as much of an oxymoron here...

Does anyone know Richard Branson's cell phone number?

Jay R. Ashworth, Baylink, The Suncoast Freenet, Tampa Bay, Florida

<http://baylink.pitas.com> +1 727 647 1274 jra@baylink.com

✶ PayPal fraud, and the importance of grammar

Geoffrey Brent <g.brent@student.unsw.edu.au>

Wed, 25 Jun 2003 13:28:49 +1000

In the last four days I've received four e-mail messages purporting to be from PayPal:

"Your (sic) As part of our continuing commitment to protect your account and to reduce the instance (sic) of fraud on our Web site, we are undertaking a period (sic) review of our member accounts. You are requested to visit our site by following the link given below."

The link is the clickable text

```
"https://www.paypal.com/cgi-bin/webscr?cmd=verification
<http://www.paypal.com@207.44.196.35/
%7Eredbarpr/cgi-bin/webscr%3fcmd=verification/>",
```

but hovering over it and looking at the URL this produces shows that the actual link is

```
http://www.paypal.com@207.44.196.35/~redbarpr/cgi-bin/webscr%
3fcmd=verification
```

Something that could very easily be mistaken for a legitimate PayPal site, no doubt set up to steal account details.

I think a very similar fraud has been reported on RISKS before, but the text illustrates an interesting point - even when the *technical* side of a scam is well-concealed, frauds often give themselves away by other signs - in this case, a poor grasp of the language. The flip-side to this is that legitimate businesses do well to maintain high standards of presentation, because it makes it easier to distinguish them from most scammers.

✶ When spam filters go bad

Monty Solomon <monty@roscom.com>
Sun, 22 Jun 2003 01:49:33 -0400

Trying to block junk mail, my cable modem company installed a system that prevented me from getting my REAL mail -- and when I complained, insisted it was all for the good of the System.

- - - - -
By Laura Miller, 19 Jun 2003

"The equivalent of treating dandruff by decapitation": That's what Frank Zappa, testifying before a Senate committee in 1985, called the censorship plans of the Parents Music Resource Center. In the annals of overreaction, draconian measures tend to spring from mind-muddling passions -- in the case of the PMRC, parental desire to protect the young from nastiness. But when it comes to passion, even our darkest, most primal instincts can hardly compare to the raw fury that people have come to feel toward spam. So e-mail users, beware: It's time to watch your head. I can testify from personal experience that the cure has finally become worse than the disease.

In June, the company that provides my cable modem service, Road Runner, installed a superaggressive new set of spam blockers on its e-mail servers. Late in the first day of the blockers' activation, I suddenly noticed that I hadn't gotten any e-mail at all in nearly three hours. No e-mail from Salon colleagues or from friends and, most puzzling of all, no e-mail from the editor at the New York Times with whom I'd been corresponding all morning about a freelance piece I was writing for her. I gave her a call. ...

<http://www.salon.com/tech/feature/2003/06/19/spamblockers/>

 New State Laws on Privacy

"Robert Ellis Smith" <ellis84@rcn.com>

Thu, 19 Jun 2003 10:52:36 -0400

Privacy Journal has published the latest supplement to its "Compilation of State and Federal Privacy Laws," showing a huge increase in state anti-spam laws and do-not-call telemarketing laws. A total of 34 states have passed new laws limiting bulk electronic-mail advertising, according to Privacy Journal's new listing, which includes a description and legal citation for each law. Most states require that "spam" be labeled as advertising and provide a means to get off an e-mail ad list. Other laws are more stringent, making some "spam" a crime or requiring an advertiser to consult a do-not-e-mail list maintained by the state.

The Compilation of State and Federal Privacy Laws 2003 Supplement lists shows 26 state laws requiring telemarketers to consult a state-maintained do-not-call list. Some state lists will be merged with a new federal database beginning in late summer this year.

The book and 2003 supplement are available for \$31 plus \$4 handling from Privacy Journal, PO Box 28577, Providence RI 02908, 401/274-7861, fax 401/274-4747, privacyjournal@prodigy.net, www.privacyjournal.net. The 2003 supplement alone costs \$21 plus \$4.

For three years, only the three states with the most intense Internet activity - California, Virginia, and Washington - had anti-spam laws, but

now nearly three-quarters of the states have enacted some limits.

Secure Coding

Monty Solomon <monty@roscom.com>

Fri, 27 Jun 2003 20:33:26 -0400

Secure Coding: Principles & Practices

By Mark G. Graff, Kenneth R. van Wyk

June 2003

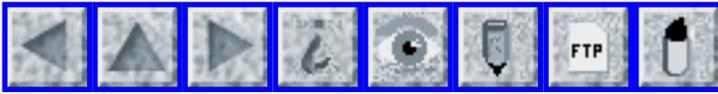
0-596-00242-4, Order Number: 2424

224 pages, \$29.95 US, \$46.95 CA, £20.95 UK

Despite their myriad manifestations and different targets, nearly all attacks on computer systems have one fundamental cause: the code used to run far too many systems today is not secure. Flaws in its design, implementation, testing, and operations allow attackers all-too-easy access. Secure Coding: Principles & Practices looks at the problem of bad code in a new way. Packed with advice based on the authors' decades of experience in the computer security field, this concise and highly readable book explains why so much code today is filled with vulnerabilities, and tells readers what they must do to avoid writing code that can be exploited by attackers.

<http://www.oreilly.com/catalog/securecdng/>

<http://www.oreilly.com/catalog/securecdng/desc.html>



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 79

Tuesday 8 July 2003

Contents

- [The risks of assuming things: German payrolls](#)
[Debora Weber-Wulff](#)
- [Radar operator's joke leads to fighter intercept](#)
[Ian Chard](#)
- ["Soft walls" will keep hijacked planes at bay](#)
[Chris Meadows](#)
[Craig DeForest](#)
- [Error in E-Mini Dow Futures creates havoc at CBOT, CME](#)
[Conrad Heiney](#)
- [\\$180 Million for Piracy Conspiracy](#)
[Monty Solomon](#)
- [Computer failure brings Hong Kong passenger to Melbourne](#)
[David Goll](#)
- [Dead-pregnant-men software failure](#)
[Ed Ravin](#)
- [Johnson Calls ATM Arrest Error 'Intolerable'](#)
[Keith A Rhodes](#)
- [RFID Site Security Gaffe Uncovered by Consumer Group](#)
[Monty Solomon](#)

- [Web site turns tables on government officials](#)
[Monty Solomon](#)
 - [FTC Increases Focus on Privacy](#)
[Bob Tedeschi via Monty Solomon](#)
 - [Web vandalism alert](#)
[NewsScan](#)
 - [Re: Cell-phone tracking](#)
[Thor Lancelot Simon](#)
 - [Microsoft Word "bytes" Tony Blair in the butt](#)
[Richard M. Smith](#)
 - [Dangers of MS Word, yet again](#)
[David Magda](#)
 - [New variant on the PayPal scam](#)
[Dawn Cohen](#)
 - [Re: Phantom voting in Israeli Knesset](#)
[Jonathan Kamens](#)
 - [Watch out for auto-dialing on cellphones](#)
[Danny Burstein](#)
 - [Glitches hit FTC 'do-not-call' list](#)
[Monty Solomon](#)
 - [Do not do not call?](#)
[Dawn Cohen](#)
 - [Risk of appropriating technology you don't understand](#)
[Doug Sojourner](#)
 - [About Do-Not-Call Lists](#)[Mark Siegel](#)
[Mark Siegel](#)
 - [Re: New State Laws on Privacy](#)
[Don Colton](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ The risks of assuming things: German payrolls

Debora Weber-Wulff <weberwu@fhtw-berlin.de>
Sun, 06 Jul 2003 23:08:26 +0200

The German government has a little problem. Up until now all of the civil servants have been paid according to a pay scale that is the same throughout Germany. The salaries are paid out by the states, but the federal government determines the pay level. The company SAP has developed payroll software for the civil service that many states in German use. When a new payscale goes into effect, they just issue a table update, and everything is fine.

Now suddenly the states are rebelling: Berlin has left the fold, and just this week concocted a wacky payment system. Certain extras are being cut, others kept, pay is being cut either 8, 10 or 12 percent depending on what scale people are in, the work week is to be decreased by 2 hours a week for most of them, etc. etc. No one really understands it, except that Berlin is broke and is trying to save money any way it can. The changes are to go into effect immediately - except that there's the slight problem with the payroll system. It assumes the same tariffs as everywhere.....

Looks like the folks down at SAP are going to have their vacations canceled, as they try to whip up programs to institute this payment schedule change.

Or as a colleague once said many, many years ago: No one can be **that** crazy.... only to discover a few months later that there really was someone with a really crazy schema for organizing stuff.

Prof. Dr. Debora Weber-Wulff, FHTW Berlin, FB 4, Internationale
Medieninformatik Treskowallee 8, 10313 Berlin +49-30-5019-2320

✶ Radar operator's joke leads to fighter intercept

"Ian Chard" <ichard@cadence.com>

Thu, 3 Jul 2003 15:27:41 +0100

Avweb Newswire

(http://www.avweb.com/newswire/9_27b/complete/185253-1.html):

"In Europe last week, French fighter jets almost shot down a civilian helicopter that wandered over Lake Geneva, after a Swiss controller jokingly labelled the helicopter as 'al-Qaeda' on his radar screen."

Ian Chard RHCE Unix systems administrator E: ichard@cadence.com
European IT, Cadence Design Systems Ltd T: +44 (0)1506 595019
The Alba Campus, Livingston, Scotland EH54 7HH M: +44 (0)7901 855073

✶ "Soft walls" will keep hijacked planes at bay

Robotech_Master <robotech@eyrie.org>
Thu, 3 Jul 2003 10:17:29 -0500

Article in *NewScientist* about an interesting new technique for keeping airliners from crashing into skyscrapers:

<http://www.newscientist.com/news/news.jsp?id=ns99993893>

The proposal suggests

modifying the avionics in aircraft so that the plane would fight any efforts by the pilot to fly into restricted airspace. So if a plane was flying with a no-fly-zone to the left, and the pilot started banking left to enter the zone, the avionics would counter by banking right. Lee's system, called "soft walls", would first gently resist the pilot, and then become increasingly forceful until it prevailed. The risks of this technique I leave as an exercise to the reader.

Chris Meadows aka Robotech_Master robotech@eyrie.org
<http://www.eyrie.org/~robotech>

✶ "Soft walls" = dangerous avionics?

Craig DeForest <zowie@euterpe.boulder.swri.edu>

Mon, 7 Jul 2003 13:03:45 -0600

Edward Lee, at U.C. Berkeley, is proposing to implement no-fly zones around skyscrapers (and avoid a repeat of the 9/11 massacre) by using GPS to override the controls of civilian aircraft. Based on a database (in the aircraft) of building locations, the on-board avionics would force the controls of large airplanes to prevent them from flying into large buildings (with presumably known locations).

There's an interesting article in this week's New Scientist (<http://www.newscientist.com/news/news.jsp?id=ns99993893>) that talks about Lee's system and relates it to other ideas for counter-terrorism. Interestingly, one advantage that Lee uses is that other systems require radio links with the ground and therefore "can be jammed, or hacked into" (while, presumably, GPS cannot?).

Not surprisingly, Lee says that pilots are "openly hostile" to the idea.

It seems to me that the system falls prey to a weakness that so many pseudo-security systems do: it's in essence a cooperative system, rather than a pre-emptive one (by analogy to multitasking in the computing world). Even assuming the avionics work flawlessly, it would be impossible to install the "soft wall" system on every airplane in the country, let alone the world -- and it only takes one airplane with the soft-wall avionics missing or disabled, to defeat the purpose of the whole system.

✶ Error in E-Mini Dow Futures creates havoc at CBOT, CME

"Conrad Heiney" <conrad@fringehead.org>

Thu, 3 Jul 2003 14:16:01 -0700

The Wall Street Journal today (7/3/03) reported that a mistaken order on the Chicago Board of Trade's "e-mini Dow Jones Industrial Average Futures" caused wild market swings today.

Apparently an order to sell 10,000 contracts instead of 100 was put in by mistake. This caused the market, which had been on the upswing that day, to plunge downwards in both the Chicago Board of Trade and the Chicago Mercantile Exchange. Several traders reported assuming that some bad news such as a terrorist attack had sparked the sell-off.

The RISK of a typo on an electronic system causing financial havoc is once again made clear.

Conrad Heiney
conrad@fringehead.org
<http://fringehead.org>

✦ \$180 Million for Piracy Conspiracy

Monty Solomon <monty@roscom.com>
Sun, 29 Jun 2003 23:39:37 -0400

\$180 million at \$500 a month, Vickie Chachere, Associated Press, 28 Jun 2003

A man who schemed to steal satellite television signals now has something much bigger than a cable bill to pay -- a whopping \$180 million restitution order on which he is to make \$500 monthly payments.

<http://www.orlandosentinel.com/news/orl-locpayback28062803jun28,0,5719929.story>
<http://yro.slashdot.org/yro/03/06/28/181227.shtml>

✦ Computer failure brings Hong Kong passenger to Melbourne

David Goll <dgoll@national.com.au>
Tue, 8 Jul 2003 11:46:04 +1000

From today's *Melbourne Age*: According to reports on local radio this morning, the lady in question was in possession of a branded boarding pass which clearly identified her carrier as Cathay Pacific not Qantas. One has to question our reliance on technology when even holding a branded boarding pass, a passenger can inadvertently walk onto the wrong flight and end up not only in a different country, but a different hemisphere to boot!

<http://www.theage.com.au/articles/2003/07/08/1057430177680.html>

✶ Dead-pregnant-men software failure

Ed Ravin <eravin@panix.com>
Mon, 7 Jul 2003 01:38:16 -0400

In a NY Times story about the effects of NY City budget cuts:

<http://www.nytimes.com/2003/07/07/nyregion/07BLOC.html?pagewanted=print>

(link free until July 13 or so, after that they charge):

Is a discussion of yet another multi-million dollar software development failure:

Eight years ago, at the urging of [...] funeral directors, the city agreed to develop a computerized registration system [for the filing of death certificates]. About \$3.2 million was spent to design one, according to an audit released on June 23 by the city comptroller. Then the plans were abandoned when the prototype system developed serious problems, like registering some men as having been pregnant when they died. The city now plans to spend \$1.8 million more for project design. The comptroller's audit called the aborted plans "a monumental waste" of taxpayer dollars.

The NYC Comptroller's press release announcing the audit is at:

http://www.comptroller.nyc.gov/press/2001_releases/01-08-055.shtm

Where it is mentioned that the city Health Department, in charge of the software development, violated both City and State procurement procedures in using an existing contract with IBM for "computer maintenance" to develop the new software system. The full bill for the system so far is more like \$9-\$10 million. The system still does not work, and the Health Department has issued a new RFP for the project that does not contain any references to the old system, so it appears they intend to throw it away.

The audit is available at:

http://www.comptroller.nyc.gov/bureaus/audit/06-23-03_7A03-073.shtm

The Comptroller quickly reaches to the heart of the matter:

"[...] the Department did not employ a formal systems development methodology or an independent software quality assurance consultant [as required by City rules, which] contributed to the apparent failure of this project."

Meanwhile, across the river in New Jersey, a similar project was completed by leveraging an existing Sybase system from the New York State Department of Health, taking only six months and \$250,000.

✶ Johnson Calls ATM Arrest Error 'Intolerable' (Re: [RISKS-22.78](#))

"Keith A Rhodes" <RhodesK@gao.gov>

Mon, 30 Jun 2003 08:25:02 -0400

<http://www.washingtonpost.com/wp-dyn/articles/A33576-2003Jun25.html>

Although this article is focusing more on the local Prince George's County police force and detective function -- which has gotten a lot of bad press here in the DC area for quite a long time -- I think the message that is being missed is that technology can give the exact

opposite result from that intended. Photographs from ATM cameras linked with ATM card usage and the system clocks are supposed to provide exact measures of events. However, if the ones using the data do not carefully collect it and interpret it correctly, then -- as this article states -- three apparently innocent people are arrested and held for 22 days. Humans cannot be completely removed from processes that have severe consequences, but the humans that are left "in the loop" must understand that what they do has severe consequences. They should, therefore, be very careful about what the "system" is telling them. In this case, the detention of the three innocent people has allowed a killer at least 22 days to get away.

RFID Site Security Gaffe Uncovered by Consumer Group

Monty Solomon <monty@roscom.com>

Tue, 8 Jul 2003 02:08:36 -0400

CASPIAN asks, "How can we trust these people with our personal data?"

CASPIAN (Consumers Against Supermarket Privacy Invasion and Numbering) says anyone can download revealing documents labeled "confidential" from the home page of the MIT Auto-ID Center Web site in two mouse clicks. The Auto-ID Center is the organization entrusted with developing a global Internet infrastructure for radio frequency identification (RFID). Their plans are to tag all the objects manufactured on the planet with RFID chips and track them via the Internet. Privacy advocates are alarmed about the Center's plans because RFID technology could enable businesses to collect an unprecedented amount of information about consumers' possessions and physical movements. They point out that consumers might not even know they're being surveilled since tiny RFID chips can be embedded in plastic, sewn into the seams of garments, or otherwise hidden. ...

http://www.nocards.org/press/pressrelease07-07-03_1.shtml

Web site turns tables on government officials

Monty Solomon <monty@roscom.com>

Sat, 5 Jul 2003 00:28:42 -0400

Hiawatha Bray, **The Boston Globe**, 4 Jul 2003

Annoyed by the prospect of a massive new federal surveillance system, two researchers at the Massachusetts Institute of Technology are celebrating the Fourth of July with a new Internet service that will let citizens create dossiers on government officials. The system will start by offering standard background information on politicians, but then go one bold step further, by asking Internet users to submit their own intelligence reports on government officials -- reports that will be published with no effort to verify their accuracy. 'It's sort of a citizen's intelligence agency,' said Chris Csikszentmihalyi, assistant professor at the MIT Media Lab. He and graduate student Ryan McKinley created the Government Information Awareness (GIA) project as a response to the US government's Total Information Awareness program (TIA). ...

<http://www.boston.com/dailyglobe2/185/business/>

[Website turns tables on government officials+.shtml](#)

FTC Increases Focus on Privacy

Monty Solomon <monty@roscom.com>

Tue, 1 Jul 2003 00:28:13 -0400

Bob Tedeschi, **The New York Times**, 30 Jun 2003

What started more than a year ago as a California teenager's quest for blue jeans ended this month with a warning shot from the Federal Trade Commission, which is moving more aggressively against e-tailers seen as too lax about protecting their customers' privacy. Online merchants say they can handle the commission's new scrutiny. But some

people, including the young man who set off the FTC investigation in this case, are not so sure. And given that the young man pointed out a security flaw in another well-known online merchant last week, he may be right.

In February 2002, Jeremiah Jacks, then a 19-year-old computer programmer, was set to buy a pair of jeans on the Web site of Guess Inc. But before entering his credit card information, he took the unusual step of checking the site's security - not the security pledge in Guess.com's privacy policy, but the company's actual practices. In the site's address bar he entered a string of characters that, on an insecure site, would produce a page listing the credit card numbers of the company's customers. The vulnerability, he said, is well known within the programming community.

It worked. About 200,000 customer names and credit card numbers appeared in Mr. Jacks's browser. In an interview last week, Mr. Jacks recalled that he had immediately tried to inform Guess of its vulnerability to such a break-in [an SQL injection]. Guess.com ignored his entreaties, he said, and Mr. Jacks soon reported his discovery to SecurityFocus, an Internet security news site owned by the Symantec Corporation, which then notified Guess. Within hours, the company fixed the site.

<http://www.nytimes.com/2003/06/30/technology/30ECOM.html>

Web vandalism alert

"NewsScan" <newsscan@newsscan.com>

Thu, 03 Jul 2003 09:30:59 -0700

Anonymous organizers of a Web-vandalizing contest this weekend say that the goal will be to deface 6,000 Web sites in six hours, with winners to be awarded prizes such as Web hosting space and Internet domain names. Pete Allor of Internet Security Systems Inc., which runs a threat-detection service, cautions Web operators: "The problem is now, and you shouldn't wait until Sunday to address it." (Atlanta Journal-Constitution 3 Jul 2003)

<http://www.ajc.com/business/content/business/0703/03hacker.html>

NewsScan Daily, 3 Jul 2003

[Apparently mostly small sites were hit. PGN]

✶ Re: Cell-phone tracking (Leshner, [RISKS-22.78](#))

Thor Lancelot Simon <tls@panix.com>

28 Jun 2003 18:17:21 -0400

Knowing which location register (cell-phone networks use, essentially, remote procedure call with callbacks between "location registers" to authorize outbound calls, correctly route inbound calls, etc.) a phone is currently active on, or has recently been active on, is **not** the same as knowing where a phone is with GPS precision, nor even the same as knowing which cell site a phone is currently speaking to. Logs of transitions between LRs ("roaming", even if that hardly exists from most customers' points of view any longer) are useful and probably even necessary for diagnosing connectivity and billing problems and for settling accounts among providers.

✶ Microsoft Word "bytes" Tony Blair in the butt

"Richard M. Smith" <rms@computerbytesman.com>

Mon, 30 Jun 2003 09:04:13 -0400

Microsoft Word documents are notorious for containing private information in file headers which people would sometimes rather not share. The British government of Tony Blair just learned this lesson the hard way.

Last week, Alastair Campbell, Blair's Director of Communications and Strategy, was in the hot seat in British Parliament hearings

explaining what roles four of his employees played in the creation of a plagiarized dossier on Iraq which the UK government published in February 2003. The names of these four employees were found hidden inside of a Microsoft Word file of the Iraq dossier which was posted on the 10 Downing Street Web site for use by the press. The "dodgy dossier" as it became known in the British press raised serious questions about the quality of British intelligence before the second Iraq war.

I wrote an article for my Web site about how a bit computer forensics Analysis played a role in this controversy:

<http://www.ComputerBytesMan.com/privacy/blair.htm>

Richard M. Smith <http://www.ComputerBytesMan.com>

⚡ Dangers of MS Word, yet again

David Magda <dmagda+risks@magda.ca>
Thu, 3 Jul 2003 20:28:52 -0400

The British government learned the hard way about how Microsoft Word documents keep a revision history:

<http://www.wsws.org/articles/2003/feb2003/cnew-f10.shtml>

<http://www.computerbytesman.com/privacy/blair.htm>

<http://www.abc.net.au/pm/s779254.htm>

The original analysis was supposedly this:

<http://www.casi.org.uk/discuss/2003/msg00457.html>

This is nothing new of course: see [RISKS 20.83](#), [20.28](#), [17.76](#), [19.97](#), [18.46](#), [18.44](#), [18.41](#), etc.

This problem goes back to (at least) 1996 ([RISKS 17.76](#)) and yet

people are still bitten by this bug(?).

The more things change...

David Magda <dmagda at ee.ryerson.ca>, <http://www.magda.ca/>

✂ New variant on the PayPal scam

"Dawn Cohen" <COHEND@wyeth.com>

Thu, 03 Jul 2003 09:23:02 -0400

I don't know exactly what it is about PayPal (as compared with any other e-commerce sort of thing)...I seem to get more scam e-mails targeting them than anything else, and all of these e-mails seem to look very similar. They all appear to be from PayPal, and include HTML forms with legitimate PayPal images and have links with real PayPal URL's. The kicker is always that the submit button takes you to a non-PayPal site.

The newest variant is a bit more insidious than the previous ones I've received. The submit button, as usual, takes you to a non-PayPal site, but appears to immediately re-direct you to a valid PayPal page. You have to either be looking in the page source for the non-PayPal URL or be *very* quick to notice that you are going to a non-PayPal URL, first. And even the non-PayPal URL might be a little hard for a naive user to catch, assuming they were fast enough to see it:

<http://www.paypal.com0011101100011010011100011100011100011010011100011100011100011010011100011100011100011010011100011100011100011@pizdatohosting.com/paypal/paypal.php>

✂ Re: Phantom voting in Israeli Knesset (Ravin, [RISKS 22.76](#))

Jonathan Kamens <jik@kamens.brookline.ma.us>

Tue, 1 Jul 2003 16:13:09 -0400

It is worth noting that the computerized voting system used by the Israeli Knesset has, as far as I know, no security whatsoever. It consists solely of a station of buttons at each Member of Knesset's (MK's) seat for him/her to use to register his/her vote. No authentication is required for casting a vote. All an MK has to do to cast someone else's vote is to lean over and push the desired button at the other MK's station.

In contrast, the electronic voting stations in the US House of Representatives require a "Vote-ID" card to be inserted before a Congressman can vote. Furthermore, there are many fewer stations than seats (Congressman line up to vote at the stations), so I suspect that the stations all have cameras trained on them throughout each vote, such that if there is suspicion of wrong-doing after a vote, it is straightforward to replay the video to find out who voted twice.

The US Senate has no electronic voting equipment -- counted votes are conducted by roll-call or paper ballot.

This is surely far from the first time that MK's have voted for each other. In fact, I find myself wondering not how this could be allowed to happen, but rather why a fuss is being made about this particular instance of it. If the Knesset really wanted to prevent it, they could do so, so it seems to me that they haven't seen it as a problem. Perhaps the culture within Israel's government is changing, such that what was previously acceptable behavior is becoming unacceptable.

⚡ Watch out for auto-dialing on cellphones

danny burstein <dannyb@panix.com>
Tue, 1 Jul 2003 04:20:35 -0400 (EDT)

RISKS has previously pointed out the awkwardness that can result from inadvertently tapping an auto-dial button on a cellphone. We now have a

burgler who will now have quite a bit of spare time to study RISKS.

Per the *NY Post* article, excerpts attached:

"It seems Boylan accidentally hit the redial button on his cell phone during a burglary - providing the break-in victim with a voice-mail recording of the crime in progress, said Detective Lt. Steve Skrynecki.

"Before the 3:20 a.m. burglary on Sunday, Boylan had called the victim's girlfriend on her cell and spoke to the victim, the detective said.

"Somehow, Boylan "inadvertently hit the redial on his cell phone" while he and his buddy ransacked the house and chatted as they grabbed a video-game player, game cartridges, a remote-controlled car and an antique bayonet, Skrynecki said.

"They had no idea their crime-scene commentary was being recorded on the girlfriend's voice mail, Skrynecki said.

<http://nypost.com/news/regionalnews/2178.htm>

✶ Glitches hit FTC 'do-not-call' list

Monty Solomon <monty@roscom.com>

Tue, 1 Jul 2003 00:47:31 -0400

Nearly one-fourth of the consumers who tried to sign up for the Federal Trade Commission's Do Not Call database haven't completed the process, the agency said Monday. The agency blames in part a series of technological glitches, including aggressive spam filtering by e-mail providers that accidentally deleted some confirmation e-mails sent by the FTC. But many consumers just haven't replied to the FTC e-mail, which is the final step in the sign-up process, said FTC attorney Eileen Harrington. [Source: Bob Sullivan, Three million consumers didn't finish sign-up process, MSNBC, 30 Jun 2003]

<http://www.msnbc.com/news/933138.asp>

⚡ Do not do not call?

"Dawn Cohen" <COHEND@wyeth.com>

Tue, 01 Jul 2003 13:27:04 -0400

I found my way to the Web site for the national Do Not Call registry, through the CDT Web site.

With great cheerfulness, I registered my two phone numbers. I followed the instructions: I entered my phone numbers and one of my e-mail addresses. I received the automatic e-mails generated by the registry Web site, and followed their instructions, which were simply to click on a link in the e-mail and print out the confirmation on the linked Web page.

"How simple!" thought I to myself. "What a blessing! With no effort at all, I am relieved of countless nuisance calls that interrupt my otherwise hectic dinner!"

"But wait a bit! How does it know that the e-mail address I entered corresponds to someone who legitimately has the rights to put my number on the Do Not Call registry? Oh well...I guess it doesn't matter...suppose I go out of my way to take someone else off the list...are they going to cry because they don't get a lot of telemarketing calls? I guess not. No problem!"

"Oh, but wait...I think I saw a 'delete registration' button..."

Yup. It works the same way. Type in a phone number and your favorite e-mail address, and you can make sure that that number is not on the do not call registry!

⚡ Risk of appropriating technology you don't understand

Doug Sojourner <dsojourner@matrixsemi.com>

Mon, 30 Jun 2003 14:51:12 -0700

Like many other people, I registered at www.donotcall.gov the other day. It seems like they are using a "validation" technique that is often used for e-mail lists: contact the e-mail given to see if it really belongs to the person trying to subscribe.

Alas, this does no good when you contact an e-mail to validate a phone number.

✶ About Do-Not-Call Lists

Mark Siegel <web@eee.org>

Sun, 29 Jun 2003 11:40:09 -0700

Assume for a moment, that do not call/do not spam lists are found to be invalid/unenforceable/unconstitutional. 'They', now, have all the valid e-mail addresses and phone numbers anyone could want.

✶ Re: New State Laws on Privacy (RESmith, [22.78](#))

Don Colton <don@colton.byuh.edu>

Sat, 28 Jun 2003 19:07:44 -1000

What are the RISKS of a do-not-call (or do-not-e-mail) list? How does this process work? Does a telemarketer purchase a copy of the do-not-call list, or does the telemarketer submit his own copy and get back a list of rejections? Since conducting surveys is apparently still allowed under the new law, will telemarketers use the do-not-call list but employ a pseudo-survey marketing tactic? Or will the free market dictate that calling the unwilling is not a

money-making proposition? Or is the list seeded with honey pots to facilitate catching violators? I find myself afraid to sign up.



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

[ACM](#) Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 80

Wednesday 16 July 2003

Contents

- [Helios loss](#)
[Peter B. Ladkin](#)
- [Error In e-mini Dow Futures creates havoc at CBOT, CME](#)
[Conrad Heiney](#)
- [A Virginia law aids identity theft victims](#)
[Michael D. Shear via Monty Solomon](#)
- [David Nelson and CAPPS II?](#)
[Rob Slade](#)
- [Man charged in e-mail stalking of anchor](#)
[Rick Jervis via Monty Solomon](#)
- [Has your PC been hijacked to spread pornography?](#)
[NewsScan](#)
- [Remotely disabling PCs as an anti-theft measure](#)
[Nick Brown](#)
- [Walk-By Hacking](#)
[Erik Sherman via Monty Solomon](#)
- [Secure eBay password changes](#)
[Scott Ehrlich](#)
- [Adobe Acrobat and PDF security: no improvements for 2 years](#)
[Monty Solomon](#)

- [Bank advises ActiveX is a security product](#)
[Charles Williams](#)
 - ["Complex" security -- what hope mere mortals?](#)
[Ben Low](#)
 - [New Kind of Snooping Arrives at the Office](#)
[Marcy Alboher Nusbaum via Monty Solomon](#)
 - [Canada and the FTC Do Not Call list](#)
[Tony Harminc](#)
 - [Washing machine does the right thing after power outage](#)
[Erik Klavon](#)
 - [Sony recalling some Vaio laptops for shock risk](#)
[Monty Solomon](#)
 - [Re: "Soft walls" = dangerous avionics?](#)
[Thomas Wicklund](#)
[Robert Woodhead](#)
 - [Re: RFID Site Security Gaffe ...](#)
[Crispin Cowan](#)
 - [Re: The risks of assuming things: German payrolls](#)
[Josef Janko](#)
 - [REVIEW: "Computer and Intrusion Forensics", George Mohay et al.](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ Helios loss

<"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>>

Wed, 16 Jul 2003 22:28:22 +0200

The Helios solar-powered flying wing was lost in June in the Pacific just west of the Hawaiian Islands, whence it was flying, due to "control difficulties that resulted in severe oscillations" at about 3,000 ft altitude [1]. The craft set an altitude record for propeller-driven craft of

nearly 100,000 ft in its previous set of flights for NASA.

Helios is (rather, was) extremely lightweight and remote-piloted. Lots of it has been recovered from the ocean, but the fuel-cell system, reported to cost \$10m, sank in about 1,800m of water and is unlikely to be recovered.

The National Research Council Committee on the Effects of Aircraft-Pilot Coupling [APC] on Flight Safety reported in 1997 that, although APC events are rare, they occur "at some point during the development of almost all FBW [Fly-By-Wire] aircraft" and notes that they are often associated with the introduction of new technologies [2, p6], of which the Helios is one of the more remarkable.

[1] Guy Norris, Helios board looks at cause of 'severe oscillations', Flight International, 15-21 July, 2003, p26.

[2] National Research Council, Committee on the Effects of Aircraft-Pilot Coupling, "Aviation Safety and Pilot Control", National Academy Press, 1997.

Peter B. Ladkin, University of Bielefeld, Germany
<http://www.rvs.uni-bielefeld.de>

🚨 Error In e-mini Dow Futures creates havoc at CBOT, CME

<"Conrad Heiney" <conrad@fringehead.org>>
Thu, 3 Jul 2003 14:16:01 -0700

The *Wall Street Journal* reported today that a mistaken order on the Chicago Board of Trade's "e-mini Dow Jones Industrial Average Futures" caused wild market swings today.

Apparently an order to sell 10,000 contracts instead of 100 was put in by mistake. This caused the market, which had been on the upswing that day, to plunge downwards in both the Chicago Board of Trade and the Chicago Mercantile Exchange. Several traders reported assuming that some bad news such as a terrorist attack had sparked the sell-off.

The RISK of a typo on an electronic system causing financial havoc is once again made clear.

Conrad Heiney conrad@fringehead.org <http://fringehead.org>

⚡ A Virginia law aids identity theft victims

<Monty Solomon <monty@roscom.com>>

Sun, 13 Jul 2003 22:25:39 -0400

By Michael D. Shear, *The Washington Post*, 13 Jul 2003

Federal and state police put the handcuffs on 32-year-old Angel Gonzales in front of his wife and two young children just as the neighborhood school bus pulled up. "We're taking your father to jail," they told his 6-year-old daughter, walking Gonzales to the cruiser as his neighbors gawked. The police had nabbed Gonzales, who lives in the Tidewater area of

Virginia, on a Las Vegas fugitive warrant on cocaine charges. The warrant said he was armed and dangerous.

Ambur Daley, 27, was arrested in a North Carolina airport as she returned from visiting her grandmother in Canada. The Staunton, Va., resident was booked, fingerprinted, and kept overnight in jail, accused of writing bad checks.

In fact, neither Daley nor Gonzales had done anything wrong. The crimes they were accused of were committed by phantoms -- identity thieves who have stolen their names, Social Security numbers, addresses, and telephone numbers. Dependent on electronic records in databanks, police across the nation were chasing the wrong people.

Both now have a Virginia Identity Theft Passport, the first two victims to participate in a program aimed at giving people such as Daley and Gonzales a fighting chance in convincing police of their innocence. A state law creating the program took effect July 1. Issued by a judge and bearing the seal of Attorney General Jerry W. Kilgore, the passport is intended to aid Virginia residents who are the victims of identity theft. ...

[http://www.boston.com:80/dailyglobe2/194/nation/
A_Virginia_law_aids_identity_theft_victims+.shtml](http://www.boston.com:80/dailyglobe2/194/nation/A_Virginia_law_aids_identity_theft_victims+.shtml)

David Nelson and CAPPs II?

<Rob Slade <rslade@sprint.ca>>
Mon, 14 Jul 2003 12:18:20 -0800

According to a story in the "This is True" mailing list, based on another from the *Los Angeles Daily News*, 6 people in the Los Angeles area, 18 in Oregon, and 4 in Alaska, all with the name David Nelson, have been pulled from commercial flights even after passing security checks. The Transportation Security Administration is quoted as saying that the name is not on any list, but that pattern matching technology is flagging the name. Does anyone have any further information on this phenomenon?

rslade@vcn.bc.ca slade@victoria.tc.ca rslade@sun.soci.niu.edu
<http://victoria.tc.ca/techrev> or <http://sun.soci.niu.edu/~rslade>

✶ Man charged in e-mail stalking of anchor

<Monty Solomon <monty@roscom.com>>
Wed, 16 Jul 2003 02:39:05 -0400

Tonny Horne, an Indiana man who thought Chicago WFLD (Channel 32) news anchor Tamron Hall was talking to him through his television set, and who showered her with affectionate and obscene e-mails for two years, will be among the first people charged under Illinois' 2001 cyberstalking law. A grand jury indicted him on charges of cyberstalking and criminal trespassing. He had been arrested on 16 Jun 2003 outside the Chicago Fox

studios. If convicted, he could face 2 to 5 years in prison.

[Source:

article by Rick Jervis, *Chicago Tribune*, 13 Jul 2003; PGN-ed]

<http://www.chicagotribune.com/technology/chi-0307130506jul13,1,2009477.story>

✶ Has your PC been hijacked to spread pornography?

<"NewsScan" <newsscan@newsscan.com>>

Fri, 11 Jul 2003 09:40:42 -0700

Computer security expert Richard M. Smith says that in the last month network vandals (possibly linked to Russian organized crime) have found ways to take over PCs with high-speed connections to the Internet and use them, without their owners' knowledge, to send Web pages advertising pornographic sites. Smith says that "people are sort of involved in the porno business and don't even know it." Most PC owners don't know when their computers have been hijacked and the hijacking apparently doesn't damage the computer or disrupt its operation. Because so many different machines are hijacked to perpetrate this scheme, there's no single computer that be shut down to end the problem. Smith adds: "We're dealing with somebody here who is very clever." (*The New York Times*, 11 Jul 2003; NewsScan Daily, 11 Jul 2003)

<http://partners.nytimes.com/2003/07/11/technology/11HACK.html>

✶ Remotely disabling PCs as an anti-theft measure

<BROWN Nick <Nick.BROWN@coe.int>>

Fri, 30 May 2003 16:04:59 +0200

ZDNet reports yet another attempt to "discourage PC theft":

http://zdnet.com.com/2100-1105_2-1009807.html

A short extract:

"Every time a computer outfitted with TheftGuard connects to the Internet, it pings the TheftGuard site. A computer-theft victim can register the machine at the site. If the stolen machine is brought online, the original owner can arrange to have the machine crippled or crippled with all data erased, and can determine the Internet Protocol address used-- which can help in hunting down the thief."

Naturally:

- The TheftGuard site can and will never, ever be hacked - or even a tempting target for hackers;
- Extensive checks will be put in place to ensure that only the registered owner of a PC can call in to say it's been stolen (perhaps they'll ask for your SSN ?);
- The world's law enforcement agencies have thousands of officers just standing by reports saying "the person who used IP address A.B. C.D at <timestamp> is a thief; go get them !".

Nick Brown, Strasbourg, France

[Now, that is nice sarcasm. PGN]

✶ Walk-By Hacking

<Monty Solomon <monty@roscom.com>>

Sun, 13 Jul 2003 12:28:15 -0400

Erik Sherman, *The New York Times*, 13 Jul 2003

'We've got 12 . . . wait, 13. Another just came in!'

On the hunt for 30 seconds, Gary Morse is jazzed. We've walked about 45 feet down Avenue of the Americas in Midtown Manhattan, and he has been counting the number of chirrups coming from the speaker of his hand-held computer. Each represents potential prey: wireless networks in the offices and apartments above us. So far, we have had more than a dozen chances to sneak Internet access, reap user ID's and passwords and otherwise peer into the private affairs of individuals and businesses.

Morse is an expert -- president of Razorpoint Security Technologies Inc., a computer security consulting firm that helps companies find their weak spots and fix them -- and a self-described 'professional hacker.' He knows dozens of tricks to ease his way into any of the networks he has found. Most users don't realize that left untended, the wireless technology that can quickly connect computers will literally broadcast every bit of transmitted information to anyone with a computer and a \$40 wireless networking card.

The software package running on Morse's hand-held is called

Kismet, from a Turkish-derived word meaning fate. The program uses the wireless card like a police band scanner, noting each wireless network that makes its presence known. 'I could put it in my pocket and record all the networks without anyone seeing,' he says. The program is available to security experts and would-be hackers for a perfectly legal and free download. ...

<http://www.nytimes.com/2003/07/13/magazine/13HACKING.html>

Secure eBay password changes

<se@panix.com (Scott Ehrlich)>

15 Jul 2003 19:31:53 -0400

[Cf. the item by Paul Festa via Monty Solomon in [RISKS-22.40](#). PGN]

<http://catless.ncl.ac.uk/Risks/22.40.html#subj3>

eBay's Web site allows for SSL (https -- i.e., secure) logins, but non-SSL (http -- i.e., insecure) password changes.

A recent visit to half.com, and eBay company, provides for SSL logins, and, to my surprise, an SSL password change screen. I promptly changed my password using half's ssl form, logged out, then logged into eBay via SSL using my new password from half.com, and it took.

So, even if eBay doesn't change their 'Change Password' form [back] to SSL, we can still use half.com's form and do it securely.

Now watch - I say this and half.com will magically remove SSL capability from its password change form.

Adobe Acrobat and PDF security: no improvements for 2 years

<"monty solomon" <monty@roscom.com>>

Tue, 8 Jul 2003 11:58:00 -0400

Software released in 2003 contains vulnerabilities disclosed in 2001

8 Jul 2003

Summary:

In early 2001, we have discovered a serious security flaw in Adobe Acrobat and Adobe Acrobat Reader. In July'2001, we've briefly described it in "eBook Security: Theory and Practice" speech on DefCon security conference. Since there was no reaction from Adobe (though Adobe representative has attended the conference), we have reported this vulnerability to CERT in September'2002 (after more than a year), still not disclosing technical details to the public. Only in March'2003, CERT Vulnerability Note (VU#549913) has been published, and after a week, Adobe has responded officially (for the first time) issuing the Vendor Statement (JSHA-5EZQGZ), promising to fix the problem in new versions of Adobe Acrobat and Adobe Reader software expected in the second quarter of 2003. When these versions became available, we have found that though some minor improvements have been made, the whole Adobe security model is still very vulnerable, and so

sent a follow-up to both CERT and Adobe. Both parties failed to respond.

Full story:

<http://archives.neohapsis.com/archives/vulnwatch/2003-q3/0011.html>

✶ Bank advises ActiveX is a security product

<Charles Williams <C.D.H.Williams@exeter.ac.uk>>

Tue, 8 Jul 2003 19:26:56 +0100

The Internet bank Egg <<http://www.egg.com/>> has just sent me an unsolicited leaflet (EP1996 06/03) trying to induce me to sign up for its account aggregation service. Step 2 of its four-step procedure says:

"Read and accept the terms and conditions. Then download a piece of software from Microsoft, called ActiveX. This acts like a digital safe and sits on your PC protecting your password and log in details."

How many of Egg's customers have now installed ActiveX in the belief that it is a security product?

✶ "Complex" security -- what hope mere mortals?

<Ben Low <ben@bdlow.net>>

Tue, 15 Jul 2003 14:18:36 +1000

The Center for the Study of Complex Systems (CSCS) at the University of Michigan appears to be staffed with competent, knowledgeable people who study "complex systems".

Yet their Computer Lab Security page at <http://www.pscs.umich.edu/lab/security.html> advises the user, when faced with a ssh host key change warning (potential "man in the middle" attack) to essentially ignore the warning, and to simply delete the offending key.

When a group studying "complex systems" has difficulty dealing with the issues of computer security, what hope to mere mortals hold?

✶ New Kind of Snooping Arrives at the Office (Marci Alboher Nusbaum)

<Monty Solomon <monty@roscom.com>>

Mon, 14 Jul 2003 21:57:44 -0400

Corporate executives are becoming increasingly aggressive about spying on their employees, and with good reason: now, in addition to job shirkers and office-supply thieves, they have to worry about being held accountable for the misconduct of their subordinates. Even one offensive e-mail message circulated around the office by a single employee can pose a liability risk for a company. Not only that, but a wave of laws - including the federal Health Insurance Portability and Accountability Act of 1996 and the

anticorruption and corporate-governance Sarbanes-Oxley Act of 2002 - have imposed new record-keeping and investigative burdens on companies. Not complying with some laws can result in the personal liability of officers and directors.

As a result, employers have stepped up their surveillance of employees, often using stealth techniques to peer deep into their computer use. As of 2001, more than a third of all American workers with access to computers, or 14 million in all, were being monitored in one way or another, according to the Privacy Foundation, a Denver research group; with added pressure on executives to oversee their employees' electronic activities, experts predict that those numbers will grow. ...

[Source: Marci Alboher Nusbaum, *The New York Times*, 13 Jul 2003]

<http://www.nytimes.com/2003/07/13/business/yourmoney/13EXLI.html>

✶ Canada and the FTC Do Not Call list

<"Tony Harminc" <tony@harminc.com>>

Tue, 8 Jul 2003 19:54:58 -0400

Curious, I went to the FTC site and tried to register my Canadian home phone number. It was rejected with an uninformative error message. However the site was quite happy to accept my (also Canadian) 800 number. This raises a

blend of techno-legal issues, because it is not possible to distinguish syntactically or in any simple way between a US and Canadian 800 number, and indeed one number can terminate in multiple locations based on the caller's location, the time of day, load, etc. So what's the legal situation if I get a junk call at this number from a US telemarketer? From a non-US one? US legislators have not been shy in the past about extending the reach of their laws outside their borders. Is this legislation written clearly enough to provide a definitive answer?

The Canadian telecom regulator (the CRTC) has been mumbling about Do Not Call for some years. Perhaps they should get together with their southern counterparts and arrange a common site and database. On second thought, maybe they should just go for a friendlier message.

⚡ Washing machine does the right thing after power outage

<Erik Klavon <erik@eriq.org>>
Tue, 15 Jul 2003 10:11:13 -0700

Readers of RISKS are now doubt familiar with some of the less than graceful ways in which technology fails in the event of a brown or black out. When the electricity to my apartment building went out recently, I thought I might experience just such a failure.

Five minutes prior to losing power, I had started a load of laundry in the

shared washing machine on my floor. The laundry machines in my complex use a smart card system for payment as opposed to coins. The machines have a digital control system that displays the remaining time and the cycle on an LCD display. After power was lost I checked the machine to verify that it had lost power. No display, not noise and no overhead light in the laundry room. I figured I was out US\$1.25, good for the recently increased bus fare in San Francisco.

When power was restored, I returned to the laundry room to find that the machine had restarted and was prompting me to select a cycle. It appears the designers had thought about the problem of losing power mid cycle and decided to start the cycle over after user input once power had been restored. This is the right thing when you consider a repair person who wouldn't want the machine starting by itself unexpectedly when power is restored after electrical work.

✶ Sony recalling some Vaio laptops for shock risk

<Monty Solomon <monty@roscom.com>>

Wed, 9 Jul 2003 22:06:16 -0400

Sony is recalling some Vaio FRV laptops because of a static-electric shock hazard, which can occur if and your phone rings whenever the laptop is plugged in and and connected to a grounded peripheral, the phone

line is disabled, and you are touching a metal part of the laptop. No injuries have been recorded, and fewer than 10 complaints. (PGN-ed from 9 Jul 2003 Reuters item)

<http://finance.lycos.com/home/news/story.asp?story=34798831>

✶ Re: "Soft walls" = dangerous avionics? (DeForest, [RISKS-22.79](#))

<Thomas Wicklund <wicklund@eskimo.com>>

Fri, 11 Jul 2003 09:43:19 -0600

The "soft walls" idea of steering planes away from restricted airspace leaves the question of what constitutes "restricted" airspace? After adding all possible terrorist targets, I can imagine a flight into a large east coast city weaving through the narrow "safe" course to the airport but leaving the airlines bankrupt paying for air sickness bags.

Of course, the airport itself is a terrorist target and should be restricted, right?

✶ Re: "Soft walls" = dangerous avionics? (DeForest, [RISKS-22.79](#))

<Robert Woodhead <trebor@animeigo.com>>

Wed, 9 Jul 2003 19:23:05 -0400

> ... and it only takes one airplane with the soft-wall avionics

missing or
> disabled, to defeat the purpose of the whole system.

Not to mention subverting the code so that at a particular date and time, the logic inverted and the exclusion zones became the only place where the airplanes would fly...

⚡ Re: RFID Site Security Gaffe ... (Solomon, [RISKS-22.79](#))

<Crispin Cowan <crispin@immunix.com>>
Tue, 08 Jul 2003 22:53:41 -0700

Hmmm ... How well do RFID embedded chips survive exposure to stun guns, cattle prods or other colorful toys?
<http://www.violetwands.com/entrance.html>

I'm not above wandng my groceries with some high voltage to preserve some privacy. Chips can be hardened, but radio chips would seem to be more difficult to harden against high voltage.

Crispin Cowan, Ph.D. <http://immunix.com/~crispin/>
Chief Scientist, Immunix <http://immunix.com> <http://www.immunix.com/shop/>

⚡ Re: The risks of assuming things: German payrolls (DWW, [RISKS-22.79](#))

<"Josef Janko" <josef.janko@web.de>>
Sun, 13 Jul 2003 15:26:31 +0200

It must be a wonderful picture imagining how thousands of software developers delay their vacations to provide a poor public servant like DWW with her paycheck in time... However, recalling my experience with the Berlin local government, the reality is not so dramatic. The payment system now is not more "wacky" than it was 28 years ago, when I first came into contact with it. Every year the government and the unions have "concocted" changes like these, and without a word the additional money has been paid one, two, or even three months later. So where is the problem, the reason for this outburst? The problem is, that for the first time after WW II in Germany public servants have to work more and get less for that - from my point of view only a fair deal under the circumstance that their jobs guaranteed. It is not a problem of IT: it is a problem of perception - being forced to face the reality outside the ivory tower.

★ REVIEW: "Computer and Intrusion Forensics", George Mohay et al.

<Rob Slade <rslade@sprint.ca>>
Tue, 15 Jul 2003 07:59:12 -0800

BKCMINFO.RVW 20030605

"Computer and Intrusion Forensics", George Mohay et al., 2003,
1-58053-369-8, U\$79.00
%A George Mohay

%A Alison Anderson
%A Byron Collie
%A Olivier de Vel
%A Rodney McKemmish
%C 685 Canton St., Norwood, MA 02062
%D 2003
%G 1-58053-369-8
%I Artech House/Horizon
%O U\$79.00 800-225-9977 fax: +1-617-769-6334 artech@artech-house.com
%O <http://www.amazon.com/exec/obidos/ASIN/1580533698/robsladesinterne>
<http://www.amazon.co.uk/exec/obidos/ASIN/1580533698/robsladesinte-21>
%O <http://www.amazon.ca/exec/obidos/ASIN/1580533698/robsladesin03-20>
%P 395 p.
%T "Computer and Intrusion Forensics"

The traditional data recovery aspect of computer forensics has been covered by Kruse and Heiser in "Computer Forensics" (cf. BKCMPFRN.RVW), and by Caloyannides in "Computer Forensics and Privacy" (cf. BKCMFRPR.RVW) (and somewhat less ably by Casey [cf. BKCMCRIN.RVW], Kovavish and Boni [cf. BKHTCRIH.RVW], Icove, Seger, and VonStorch [cf. BKCMPCRM.RVW], Marcella and Greenfield [cf. BKCYBFOR.RVW], van Wyk and Forna [cf. BKINCRES.RVW], and Mandia and Procise [cf. BKINCDRS.RVW]).

So far network forensics has only been specifically dealt with in the not-terribly-useful "Hacker's Challenge," by Schiffman (cf. BKHKRCHL.RVW).

"Computer and Intrusion Forensics" is the first attempt to bring both topics into a single book. (It is intriguing to note that Eugene Spafford, who

wrote the foreword, is a pioneer of the "third leg": software forensics, which the book does not cover.)

Chapter one is an introduction to computer and network (intrusion) forensics, pointing out the ways that computers can be involved in the commission of crimes and the requirements for obtaining and preserving evidence in such cases. While the material provides a good foundation, the text is inflated in many places, and could benefit from stricter adherence to the topic and more focused writing. (One illustration shows a pattern of concentric rings indicating that the set of productive activities encompasses all legal endeavors which, in turn, encompasses all approved actions. I suspect that a great many legal and even approved activities are unproductive--while no doubt a number of illegal activities would be approved, at times.) "Current Practice," in chapter two, is a broad overview of the concerns, technologies, applications, procedures, and legislation bearing on digital evidence recovery from computers. In fact, this single chapter is the equivalent of, and sometimes superior to, a number of the computer forensics books mentioned above. However, the breadth of the discussion does come at the expense of depth. This content is quite suitable for the information security, or even legal, professional who needs to understand the field of computer forensics, but it does not have the detail that a practitioner may require. Although chapter three is supposed to deal with computer forensics in law enforcement (and there is a

brief section on the rules of evidence), it is primarily a reiteration (and some expansion) of the procedures for data recovery and the software tools available for this task. Forensic accounting, and the algorithms that can be used to detect fraud, are outlined in chapter four, but very little is directly relevant to computer forensics as such. Case studies, demonstrating the techniques discussed earlier and some that are not, are described in chapter five. Intrusion forensics concentrates on intrusion detection systems (IDS), although it does not provide a very clear or complete explanation of the distinctions in data collection (host- or network-based) or analysis engines (rule, signature, anomaly, or statistical). Chapter seven finishes off the book with a list of computer forensic research which is being, or should be, undertaken.

While the computer forensic content is sound, and it is heartening to see other fields being included, the very limited work on network forensics is disappointing. This text is a useful reference for those needing background material on forensic technologies, but breaks no new ground.

copyright Robert M. Slade, 2003 BKCMINFO.RVW 20030605
rslade@vcn.bc.ca slade@victoria.tc.ca rslade@sun.soci.
niu.edu
<http://victoria.tc.ca/techrev> or <http://sun.soci.niu.edu/~rslade>



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

[ACM](#) Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 81

Sunday 20 July 2003

Contents

- [Reassembly of shredded documents](#)
[Richard M. Smith](#)
- [SEVIS foreign students database](#)
[Thomas Dzubin](#)
- [IPv6 addresses too big to fit?](#)
[Joe Loughry](#)
- [Italian naming problem](#)
[Darryl Luff](#)
- [GPS-piloted tractors?](#)
[Conrad Heiney](#)
- [Health Commissioner's anonymised case reports not so anonymous](#)
[Don Mackie](#)
- [Privacy rights under threat by lawmakers](#)
[Dan Gillmor via Monty Solomon](#)
- [Carjacker tracked and bugged by Tele-Aid operator](#)
[Jonathan Epstein](#)
- [Samsung Electronics bans camera phones from key factories](#)
[Ferdinand John Reinke](#)
- [Software helps police draw crime links](#)
[Gareth Cook via Monty Solomon](#)

- [AOL blocking e-mail from other ISPs](#)
[David E. Ross](#)
 - [Lack of Abbey National telephone banking security](#)
[Adam Laurie](#)
 - [HighGroup Listing of SSN's](#)
[Alice K. Whitfield](#)
 - [Why are spammers backing spam-control laws?](#)
[NewsScan](#)
 - [California court rules against Intel in spam case](#)
[Elinor Mills Abreu via Monty Solomon](#)
 - [Re: Virginia Identity Theft Passport](#)
[John Sinteur](#)
 - [Re: David Nelson and CAPPS II?](#)
[Arthur Flatau](#)
 - [Re: Error In e-mini Dow Futures creates havoc](#)
[Stewart C. Russell](#)
 - [Re: Washing machine does the right thing after power outage](#)
[Kurt Thams](#)
 - [Re: The nuking of RFID chips](#)
[Kevin G. Rhoads](#)
 - [Formal Methods 2003 - Call for Participation and Programme Details](#)
[Diego Latella](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ Reassembly of shredded documents

<"Richard M. Smith" <rms@computerbytesman.com>>

Thu, 17 Jul 2003 12:51:45 -0400

Throughout the 1980s, Sascha Anderson, a poet, musician, and literary impresario, was one of the leading voices to speak out against the East German government and its dreaded secret police, the Stasi. But his

credibility gradually evaporated after the Communist government's collapse

as rumors about him acquired the weight of proof: he had been informing on

his dissident compatriots all along.

It turns out that his supposedly unretrievable Stasi file was *manually*

reconstructed from bags of papers that had been shredded during the final

days of the regime in 1989. However, the German government is now planning

on reconstituting 16,000 bagsful from that era, using advanced scanning

technology. [Source: Picking Up the Pieces, By Douglas Heingartner, *The

New York Times*, PGN-ed]

<http://www.nytimes.com/2003/07/17/technology/circuits/17shre.html>

[?pagewanted=all&position=](#)

[The programming effort is certainly an interesting application!]

SEVIS foreign students database

<Thomas Dzubin <dzubint@vcn.bc.ca>>

Wed, 9 Jul 2003 05:49:23 -0700 (PDT)

Under new United States homeland security laws, all U.S. schools have to

register their foreign students in the database, known as the Student and

Exchange Visitor Information System (SEVIS). This system has all the

attributes of a big system rushed into production before sufficient testing

could take place. In my mind, the RISK-iest thing about this story is that

the effects of the problems can cause life-changing situations for people including being jailed and/or deported.

Many problems with this system are detailed in the story including files being mysteriously deleted or "misplaced". Some advisers are telling students not to go back to their home countries on school breaks, in case SEVIS accidentally deletes their records. Students who are not in the system cannot re-enter the country. One quote from the story: "Daily interactions with SEVIS have become a test of wit and will"

Other bugs/glitches/problems reported:

- Unable to modify existing records which is a problem if a foreigner (or spouse) has a baby.
- extreme system slowness and random crashing
- insufficient or inadequate help desk technician support

One final quote from the story:

"The technical failings of SEVIS and the difficulty the government has had in implementing it undermine its security potential, Cotten says. If the American people feel safer because of SEVIS, then they are severely misled, she says."

Source:

<http://www.govexec.com/dailyfed/0703/070303h1.htm>

(Hopefully this link is still active. If not, Government Executive Magazine does keep old stories archived under a slightly different URL naming convention...the title "Foreign student tracking system called inefficient, intrusive" should stay the same.)

⚡ IPv6 addresses too big to fit?

<"Loughry, Joe" <joe.loughry@lmco.com>>

Thu, 17 Jul 2003 17:36:27 -0600

In light of the recent announcements by the U.S. Department of Defense in support of IPv6, we have been going through our software making the necessary changes. I found several examples of text input fields that were too short to hold a valid IPv6 address like 3ffe:1800:0:3:290:27ff:fe14:cdee.

Also necessary was replacing calls to the standard library functions `inet_ntoa()` and `inet_addr()`, among others, which do not support IPv6.

On an encouraging note, however, I found that throughout the source code, extremely conservative coding practices and good error checking everywhere means that our software does not crash when handling IPv6 addresses.

It's Y2K all over again.

Joe Loughry, Lockheed Martin Space and Strategic Missiles,
RADIANT MERCURY

⚡ Italian naming problem

<Darryl Luff <dluff@iitscdm.com.au>>

Fri, 18 Jul 2003 12:41:33 +1000

Hmm, the simple risk of your perfectly sensible domain name being interpreted very differently in other languages. [NOTE: text not mine. DL]

At least they should then have created a brilliant logo.....

If you were a company called Powergen and you had a subsidiary that operated in Italy, what would you call that company's Web site?.

Probably not <http://www.powergenitalia.com>

But they really did. ...

[A high-strung multilingually interpretable literal string!
PGN]

GPS-piloted tractors?

<"Conrad Heiney" <conrad@fringehead.org>>

Fri, 18 Jul 2003 16:28:41 -0700

According to a Reuters report on CNN today, a University of Queensland researcher is promoting an Australian technology for satellite-guided tractors. These are said to be accurate to 2 cm. Apparently advantages to these are that the tractors are more accurate and do not crush the soil as much as conventional people-driven equipment, allowing higher yield. As a bonus, they could be run at night.

<http://www.cnn.com/2003/TECH/science/07/18/satellite.tractor.>

reut/index.html

The RISK of unmanned vehicles relying on GPS signals, with or without rotating blades attached, is interesting to contemplate, especially at night!

Conrad Heiney <http://contentgoeshere.com/> <http://fringehead.org>

✶ Health Commissioner's anonymised case reports not so anonymous

<Don Mackie <donald@iconz.co.nz>>

Wed, 9 Jul 03 19:32:37 +1200

The New Zealand Health & Disability Commissioner has been dealing with complaints about health care for almost ten years. As it says at the website (www.hdc.org.nz) the purpose... is to promote and protect the rights of health and disability consumers, and to facilitate the fair, simple, speedy, and efficient resolution of complaints.

The Commissioner investigates complaints. Often there are useful lessons to be learned from the complaint and the findings, after removal of all identifying features, are published so that others can benefit. Some are posted on the website in a range of formats: html, pdf and Word document. Some of you will see where this is leading.

A colleague of mine was startled to be told by a patient that a Google search on the doctor's name yielded the text of a HDC finding as

the top
hit. While my colleague acknowledges that there was a complaint
about them
they have learned from it and believed that the publication was
anonymous.
On opening the link from Google, I got a Word document. Sure,
the names of
the individuals had been removed from the text of the document,
but when I
went Properties -> Summary, there they were. Waiting to be
found by a
search engine. I looked at a few other .doc files and the same
problem
existed. I informed the HDC and they have now pulled the .doc
opinions.

Ignorance of the hidden information in word processing files is,
of course,
not new. This one has had the potential to damage reputations
when the HDC's
office has been careful, but not careful enough, to protect them
in the
past.

Privacy rights under threat by lawmakers

<Monty Solomon <monty@roscom.com>>

Sun, 13 Jul 2003 20:23:54 -0400

Dan Gillmor, *San Jose Mercury News*, 13 Jul 2003

In the constant battle to preserve what's left of our privacy
and roll back
some of the invasions we've already suffered, one reality is all
too clear:
Elected officials are not on our side. Last week brought the
latest
perversion of the public will, the cowardly refusal of the
California

Legislature to enact even modest improvements in financial privacy. The voters will do it instead, in a ballot measure next year.

Meanwhile, state and federal lawmakers are almost totally oblivious to future threats, including some that should be dealt with before they cause trouble. For example, retailers will soon be installing little identifying radios, a technology known as RFID, into items they sell, enabling a host of new privacy invasions that could make the status quo seem benign.

We all understand why lawmakers hold the public good, and will, in such contempt. They tend to vote on behalf of their financial benefactors. Commercial interests see our privacy as a barrier to their business.

Game over? No. We have to care enough to take matters into our own hands. Pressuring politicians is vital, but it's plainly not enough. We'll need to do a little multitasking to retrieve our right to be left alone. ...

<http://www.siliconvalley.com/mld/siliconvalley/6293890.htm>

✶ Carjacker tracked and bugged by Tele-Aid operator

<Jonathan Epstein <Jonathan_Epstein@nih.gov>>

Thu, 17 Jul 2003 13:23:16 -0400

A quick-thinking bystander realized that police could track the movements of a carjacker who sped off with two small children in the back

seat. The police were able to indirectly both track and listen-in on the car, and learn that the kids in the back seat were OK.

<http://www.washingtonpost.com/wp-dyn/articles/A2862-2003Jul16.html>

Marc Fisher of the Washington Post writes:

That carjacking the other night raises some fascinating questions. I'm sure the mom was tremendously relieved that the operators in Dallas were able to listen in on her children as their kidnapper hurtled along Rt. 50 -- and goodness knows what might have happened if the Mercedes version of OnStar, called Tele-Aid, hadn't been tracking the thug's movements. But do any of you have concerns about the ability of Tele-Aid and similar companies to turn on the microphone remotely and listen in on the goings-on in your car? Or does this case prove that such privacy fears are outweighed by the good those devices can do?

⚡ Samsung Electronics bans camera phones from key factories

<"Ferdinand John Reinke" <ferdinand.john.reinke@att.net>>

Mon, 7 Jul 2003 15:45:55 -0400

Samsung Electronics is restricting use of camera phones at key factories and research centers to preclude industrial espionage. (Camera phones have become popular in South Korea.) [Source: Yahoo News, 7 Jul 2003] <http://news.yahoo.com/news?tmpl=story2&cid=1509>

[_&u=/afp/20030707/tc_afp/
skorea_samsung_it_company_030707080259&printer=1](mailto:skorea_samsung_it_company_030707080259&printer=1)

[I wonder if they remember that PDA's have camera capability?
Wonder if
financial institutions have thought about this "risk"? Not
likely. JohnR]

Software helps police draw crime links

<Monty Solomon <monty@roscom.com>>
Fri, 18 Jul 2003 02:13:53 -0400

The Boston Police Department is rolling out a powerful new computer program built to find hidden connections among people and events almost instantly, allowing detectives to investigate murders, rapes, and other crimes far faster than they can today. Called "Coplink," the program sifts through tens of millions of police records, from 911 calls to homicide investigations, to deliver a short list of potential leads in just seconds. The same kind of searching currently takes hours or even days of a detective's time -- when it is possible at all. Designed in an Arizona AI lab, Coplink searches through arrest records, incident reports, and emergency phone calls to identify potential suspects and compile all possible leads on them, including past addresses, weapons they have owned, and even the arrest records of people with whom they have been stopped in a car. In Boston, it will search only through city police records, though it

could later be expanded to stretch far more broadly. ...
[Source: Gareth Cook, *The Boston Globe*, 17 Jul 2003; PGN-ed]
[http://www.boston.com/dailyglobe2/198/nation/
Software_helps_police_draw_crime_links+.shtml](http://www.boston.com/dailyglobe2/198/nation/Software_helps_police_draw_crime_links+.shtml)

✶ AOL blocking e-mail from other ISPs

<"David E. Ross" <david@rossde.com>>

Sat, 19 Jul 2003 12:30:11 -0700

AOL has been bouncing E-mail messages from other ISPs. In their attempt to block spam, they are blocking mail servers that they presume are on end-user IP addresses. For some reason, some ISP mail servers -- including at large, well-run ISPs -- were considered to be among those addresses.

The problem started on Tuesday, 15 July, or earlier. AOL apparently did not know of the problem until a customer of an affected ISP complained on the morning of Friday, 18 July. AOL's response is that they will not be able fix the problem until Monday, 21 July, or later.

This seems to be another case of implementing technology without sufficient testing. However, the fact that a problem reported on Friday cannot be fixed until Monday indicates this risk arises from placing business considerations ahead of either technology or customer service.

David E. Ross <<http://www.rossde.com/>>

⚡ Lack of Abbey National telephone banking security

<Adam Laurie <adam@algroup.co.uk>>

Fri, 18 Jul 2003 10:41:16 +0100

I hold an Abbey National account in the joint names of myself and my wife, but my wife's entry is still in her maiden name (so from the bank's perspective it could be any individual with no special legal relationship). This account was created many moons ago, before we were married, to facilitate the purchase of a flat. After the transaction, there were a couple of hundred pounds left in the account, which have languished ever since. We recently moved house and so this account came to our attention when the tenants at the previous address forwarded our bank statements to us.

And now the scary bit...

Armed only with the statement passed to me by said 3rd party, I was able to call up the online bankers, cancel all the cheques and have all the funds in the account transferred to an arbitrary account (in this case my personal account - i.e. not a joint account with my wife).

The "extra security" questions I was asked were:

1. who is the other named account holder? (this was printed on the back of statement).
2. what is your overdraft limit? (this was printed on the front of the statement).

As the nice kid in Terminator 2 says... "easy money"... :)

Adam Laurie, A.L. Digital Ltd., The Stores, 2 Bath Road, London
W4 1LT UK

<http://www.aldigital.co.uk> <http://www.thebunker.net> Tel: +44
(20) 8742 0755

✶ HighGroup Listing of SSN's

<"Alice K. Whitfield" <qccorp@sprintmail.com>>

Fri, 18 Jul 2003 10:36:05 -0400

The risks of using social security numbers as personal identifiers in the U.S. is better known to members of this community than perhaps any other. You may appreciate then, better than the Social Security Administration apparently does, the increased risk that arises when the SSA's own published list of valid (partial) numbers contains errors of omission (<http://www.ssa.gov/foia/highgroup.htm>, as of 18 July 2003 at 1400 UT).

The errors in the July list are not numerous, and may affect mostly elderly, former railroad workers. In past instances, the errors were more widespread but eventually fixed. They show no sign of responding to any communications about the current problems, however. Obviously, the current list was not verified before the page went live.

Luckily, flunking a flawed social security number verification test

under the current regime of Total Awareness, "is not a basis ... for ... adverse action ... such as laying off, suspending, firing, or discriminating against an individual..." So, according to the Social Security Administration, no one should have to worry about those risks, at least.

✶ Why are spammers backing spam-control laws?

<"NewsScan" <newsscan@newsscan.com>>

Fri, 18 Jul 2003 09:26:46 -0700

Bigtime spam-mongers and junk-mail proponents like the Direct Marketing Association are backing proposed antispam legislation, while consumer and public-interest groups, almost without exception, oppose the bills. What's going on? "It's a sign of who benefits from these bills and who doesn't," says a spokesman for the Coalition Against Unsolicited Commercial Email. "When you see some of the biggest spammers in the country backing legislation that is allegedly antispam, you really need to wonder about what these bills actually do." The answer is that rather than banning all unsolicited e-mail outright, as many consumer groups wish, they legitimize spam, as long as the perpetrators adhere to certain rules, such as using accurate subject lines and valid return addresses, and allowing recipients to opt out of future mailings. Two bills are currently making their way through Congress and a variant of thereof is expected to pass overwhelmingly

and be signed into law later this year. [*Wall Street Journal*,
18 Jul
2003; NewsScan Daily, 18 Jul 2003]
<http://online.wsj.com/article/0,,SB105848273351539900,00.html>
(sub req'd)

California court rules against Intel in spam case

<Monty Solomon <monty@roscom.com>>
Mon, 30 Jun 2003 23:07:18 -0400

The California Supreme Court on 30 Jun 2003 ruled spammers cannot be sued under state law for property trespass for just sending e-mail -- a setback for Intel Corp., which had sued a former engineer for sending e-mails to up to 35,000 company workers. The 4-3 ruling reversed a lower court order prohibiting former Intel engineer Ken Hamidi from sending e-mails critical of Intel to thousands of its employees. Intel claimed the e-mails had trespassed on its private network and had harmed the company by reducing worker productivity. But the California Supreme Court found that Intel's computer system had not been damaged as a result of the e-mails and, therefore, there was no trespass. The court declined to expand state common law covering property trespass to apply to e-mail whose contents may be objectionable, but which is otherwise harmless. ... [Source: Elinor Mills Abreu, Reuters, 30 Jun 2003]

<http://finance.lycos.com/home/news/story.asp?story=34677087>

✶ Re: Virginia Identity Theft Passport ([RISKS-22.80](#))

<John Sinteur <john@sinteur.com>>

Thu, 17 Jul 2003 07:45:56 +0200

I can't help but wonder, how long until identity thieves won't just acquire a driver's license, credit cards, etc, with their freshly stolen identity, but one of these passports as well? Which will be relative unknown to the cop on the street, so the first few yours you could hack something together yourself in Photoshop as well...

If there's a bug in the way people use paperwork to assert and use identities, how is more paperwork going to solve that?

[Similar comment from Michael Hartley. PGN]

✶ Re: David Nelson and CAPPs II? (Slade, [RISKS-22.80](#))

<"Arthur Flatau" <arthur.flatau@amd.com>>

Thu, 17 Jul 2003 09:44:12 -0500

There was a story on this in the *Austin American Statesman* (originally from the *Chicago Tribune*).

http://www.statesman.com/insight/content/auto/epaper/editions/sunday/insight_f3e0169a836a10f00085.html

There are at least two David Nelsons in the Austin area. The articles

states:

The family [Dr. David and Cindy Nelson of Austin and their two young children] plans to fly to Canada in August, and this time they're planning countermeasures. They'll try buying David Nelson's airline ticket under D. Austin Nelson.

That is surely a tactic that the bad guys would never figure out!

Arthur Flatau, Texas Microprocessor Division, Advanced Micro Devices,
5900 East Ben White Boulevard, Austin TX 78741 Arthur.Flatau@amd.com

✶ Re: Error In e-mini Dow Futures creates havoc ([RISKS-22.80](#))

<"Stewart C. Russell" <scruss@sympatico.ca>>
Fri, 18 Jul 2003 10:17:40 -0400

It seems that typos are quite common on trading systems. Talking to a friend who is a foreign exchange trader, I found out that such misquotes are commonly called "wrong big figure" quotes.

A casual web search on this phrase will return an alarmingly large number of documents from forex houses. These documents pertain to their liability -- or lack of it -- for such quotes.

Surely we need to work on the ergonomics of such trading systems?

⚡ Re: Washing machine does the right thing after power outage

<"Kurt Thams" <thams@thams.com>>

Thu, 17 Jul 2003 10:54:38 -0700

On the other hand, an enterprising user could pull the power plug at nearly the end of the job, load a new batch of clothing, and get his second (and third and fourth...) wash free!

⚡ Re: The nuking of RFID chips (Cowan, [RISKS-22.80](#))

<"Kevin G. Rhoads" <Kevin.Rhoads@Dartmouth.EDU>>

Thu, 17 Jul 2003 09:20:25 -0400

Most stun guns and cattle prods use current limited high voltage DC. It is easy to provide overload protection for this kind of electrical insult -- although I doubt that RFID manufacturers will include such protection in the early designs. However, if such deactivation becomes common and problematic, it can be designed around.

Better to use a low output Tesla coil, which generates high voltage splattered all over the RF spectrum. Of course, a linear RF power amp driven by an RF sweep generator should also work -- but that level of equipment is not readily available. Cheap Tesla coils can be easily homebrewed and Edmund Scientific carries a model for about \$120 that is ideal.

✦ Formal Methods 2003 - Call for Participation and Programme Details

<Diego Latella <Diego.Latella@isti.cnr.it>>

Fri, 18 Jul 2003 09:58:48 +0500

The 12th International FME Symposium

Pisa, Italy - September 8-14, 2003

<http://fme03.isti.cnr.it> - fme03@isti.cnr.it

FM 2003 is the twelfth in a series of symposia organized by Formal Methods

Europe, an independent association whose aim is to stimulate the use of, and

research on, formal methods for software development. These symposia have

been notably successful in bringing together a community of users,

researchers, and developers of precise mathematical methods for software

development as well as industrial users.

Formal methods have been controversial throughout their history, and the

realization of their full potential remains, in the eyes of many practitioners, merely a promise. Have they been successful in industry? If

so, under which conditions? Has any progress been made in dispelling the

skepticism that surrounds them? Are they worth the effort? Which aspects of

formal methods have become so well established in the industrial practices

to lose the "formal method" label in the meanwhile?

FM 2003 aims to answer these questions, by contributions not only from the

Formal Methods community but also from outsiders and even from

skeptical

people who are most welcome to explain, document, and motivate the source of their reluctance.

FM 2003 will host 7 Workshops, 8 Tutorials and 1 Day dedicated to the Industry besides the 3 days of the FME Symposium. Tool demonstrations will also take place during the symposium, with the opportunity of holding presentations for each tool.

For full details on the Symposium organization and to register please go to the web site <http://fme03.isti.cnr.it>, or send your query to fme03@isti.cnr.it.

Dott. Diego Latella, Consiglio Nazionale delle Ricerche, ISTI
Via G. Moruzzi, 1 - I56124 Pisa, ITALY
phone +39 0503152982 or +39 348 8283101 fax +39 0503138091 or
+39 0503138092
Diego.Latella@isti.cnr.it <http://www.isti.cnr.it/People/D.Latella>



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

[ACM](#) Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 82

Sunday 27 July 2003

Contents

- [Serious flaws in electronic voting systems](#)
[NewsScan](#)
- [South Africa bank Internet spyware and fraud](#)
[Heinz M. Kabutz](#)
- [Stealing passwords from Kinko's](#)
[John F. Whitehead](#)
- [New method cracks passwords in seconds](#)
[NewsScan](#)
- [Bypassing the safeguards](#)
[Mark Lutton](#)
- [Limit to stupidity? Credit card scam uses rather nasty flaw.](#)
[Gillian Brent](#)
- [Biometrics technology: not yet ready for primetime](#)
[NewsScan](#)
- [Spammers who don't read RISKS](#)
[Diamond](#)
- [Adieu to 'e-mail'?](#)
[NewsScan](#)
- [E-mail harvesting and re-use as a new virus vector?](#)
[Jim Garrison](#)

- [Identity theft: a crime that pays?](#)
[NewsScan](#)
 - [Cross *words*?](#)
[Mark Brader](#)
 - [Presidential "doublespeak" ...](#)
[Jim Bauman](#)
 - [Owner of stolen 'sex.com' can sue VeriSign](#)
[Monty Solomon](#)
 - [Another risk of decency filters](#)
[J. Lasser](#)
 - [SCO wants licensing fees from corporate Linux users](#)
[Monty Solomon](#)
 - [Microsoft rediscovers MultiLevel Security](#)
[Jeremy Epstein](#)
 - [Re: Powergenitalia](#)
[Elijah Grabbet](#)
 - [Re: Error in E-Mini Dow Futures creates havoc at CBOT, CME](#)
[Greg Compestine](#)
 - [Re: GPS-piloted tractors?](#)
[Kent Borg](#)
 - [Re: GPS-piloted tractors? Hell yes! Que Stephen King!](#)
[Fredric L. Rice](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✂ **Serious flaws in electronic voting systems**

<"NewsScan" <newsscan@newsscan.com>>

Thu, 24 Jul 2003 09:28:33 -0700

Johns Hopkins University experts say that high-tech voting machine software from Diebold Election Systems has flaws that would let voters cast extra votes and allow poll workers to alter ballots secretly. Aviel D. Rubin,

technical director of the Information Security Institute at Johns Hopkins, led a team that examined the Diebold software, which has about 33,000 voting machines operating in the United States. Adam Stubblefield, a colleague of Rubin's, said that "practically anyone in the country -- from a teenager on up -- could produce these smart cards that could allow someone to vote as many times as they like." Diebold has not seen the Institute's report and would not comment on it in detail, but a company spokesman said: "We're constantly improving it so the technology we have 10 years from now will be better than what we have today. We're always open to anything that can improve our systems." Peter G. Neumann, an expert in computer security at SRI International, said the Diebold code was "just the tip of the iceberg" of problems with electronic voting systems.

[*The New York Times, 24 Jul 2003; NewsScan Daily, 24 Jul 2003]
<http://partners.nytimes.com/2003/07/24/technology/24VOTE.html>

South Africa bank Internet spyware and fraud

<"Dr. Heinz M. Kabutz" <heinz@javaspecialists.co.za>>
Mon, 21 Jul 2003 08:42:44 +0200

ABSA, the leading bank in South Africa has very weak Internet security. All you have to know is someone's bank account number and their pin, and you can set up beneficiaries, pay money over, to your heart's content. There is no TAN like in German banks. This story is not surprising at all,

what is
surprising is that it took so many years for this to happen on
such a big
scale.

Here is the story according to the Sunday Times. Simple spyware
was
installed on victim's computers and the account numbers and PIN
sent back to
the perpetrator. This allowed the thief to steal approximately
R500,000
(about US\$ 65000) from various victims.

<http://www.sundaytimes.co.za/2003/07/20/news/news01.asp>

The bank responded with the usual tips:

[http://www.absa.co.za/ABSA/Media_Releases/
Article_Page/0,1551,424,00.html](http://www.absa.co.za/ABSA/Media_Releases/Article_Page/0,1551,424,00.html)

These were the funniest:

* Make sure that the software that is loaded onto your PC via a
third party
is licensed. (How would that make a difference?)

* Update your operating system and browser with the latest
Microsoft patches
to protect your PC from exploitation. These can be downloaded
from the
Microsoft website <http://www.microsoft.com> (Assuming of course
that everyone
in South Africa uses Microsoft - oh, all the victims used
Microsoft!)

I am fairly confident that the police will catch the thief. You
cannot
transfer money out of the country from South Africa without
special
clearance, so at least we did not have the problem with money
ending up in
some country that would not cooperate.

He will probably be given a death sentence. (Not directly, but
a visit to

our jails is akin to a death sentence through HIV infection :-(

Dr. Heinz M. Kabutz (Maximum Solutions), Author of "The Java(tm) Specialists' Newsletter" <http://www.javaspecialists.co.za> +27 (83)340-5633

Stealing passwords from Kinko's

<"John F. Whitehead" <jfw@well.com>>

Sat, 26 Jul 2003 12:41:31 -0700

For two years a man stole passwords from customers in New York City Kinko's copy/printing/office services stores, and used the information to try to access and open bank accounts:

"In pleading guilty to computer damage, [Jujul] Jiang admitted that,

between February 14, 2001, and December 20, 2002, without the permission

of Kinko's Inc., he installed special keylogging software on computer

terminals located at Kinko's stores throughout Manhattan to surreptitiously record keystroking activity on those computers, and

collect computer usernames and passwords of Kinko's customers.

Jiang also admitted that he then used the confidential information he

obtained to access, or attempt to access, bank accounts belonging to other

persons, and fraudulently open on-line bank accounts.

Jiang also pled guilty to similar fraudulent conduct that he continued to

commit while on bail after his arrest on December 20, 2002."

For more see the Dept of Justice press release:

<http://www.cybercrime.gov/jiangPlea.htm>

✶ New method cracks passwords in seconds

<"NewsScan" <newsscan@newsscan.com>>

Wed, 23 Jul 2003 08:48:41 -0700

A senior research assistant at the Swiss Federal Institute of Technology's Cryptography and Security Laboratory has published a paper outlining a way to speed up the process of cracking alphanumeric Windows passwords to only 13.6 seconds on average. The previous average time was 1 minute, 41 seconds. The new method uses massive lookup tables to match encoded passwords to the original text entered by a person, thus reducing the time it takes to break the code. "Windows passwords are not very good," says researcher Phillippe Oechslin. "The problem with Windows passwords is that they do not include any random information." The only requirement for the cracker is a large amount of memory in order to accommodate the lookup tables. The larger the table, the shorter the time it takes to crack the password. Users can protect themselves by adding nonalphanumeric characters to a password, which adds another layer of complexity to the process. Any cracker would then need more time or more memory or both to accomplish the break-in. For more information on Oechslin's method, check out http://lasecwww.epfl.ch/php_code/publications/search.php?

[ref=Oech03](#) [CNet

News.com 22 Jul 2003; NewsScan Daily, 23 Jul 2003]

http://news.com.com/2100-1009_3-5053063.html

✶ Bypassing the safeguards

<Mark Lutton <mlutton@rcn.com>>

Thu, 24 Jul 2003 23:48:51 -0400

On 23 Jul 2003, New York City Councilman James E. Davis was shot to death by political opponent Othneil Boaz Askew inside New York's City Hall. Davis had a concealed handgun of his own.

How did the two opponents get their weapons past the metal detectors?

According to the news report, the councilpersons (and apparently their guests) routinely bypass the detectors.

You can have all the technology in the world against violence and terrorism and it won't do you a damn bit of good if you let everybody and his enemy go around it.

✶ Limit to stupidity? Credit card scam uses rather nasty flaw.

<Gillian Brent <reynardo@pnc.com.au>>

Fri, 25 Jul 2003 23:19:17 +1000

The following Spam arrived on the alt.devilbunnies newsgroup. As we are

fairly used to a couple of certain rabbits trying to pull similar schemes, we weren't fooled - but I'm sure some people were.

> Finally I found a hack that really works to get free VALID CREDIT CARD
> NUMBERS! I bought the information off ebay for \$15.00.
> Using a valid credit card account, you can get many more VALID CREDIT CARD NUbers for free using my method.
>
> You basically send a coded message to the yahoo account information computer database.
> All the account information still active is in this computer. Iam not going to explain exactly how it works(its around 7 pages long), I'll just tell you a little and how to do it.
>
> Copy the information below in its exact format or it will not work.
> Make sure to put a zero under each character(number, letter, hyphen, etc) you type. Type in small caps. If you capitalize, it will not work.
> And if you do not send the exact information on the credit card, it will not work. The computer has to register the information to be valid before it will send you an account. I've tried to use a false account, it doesn't work.

(I very much doubt whether this information actually came from eBay.)

I'm not going to insult your intelligence with the rest of this, but apart from the risk of losing control of your own credit card, it seems to be using a vulnerability in the yahoo system.

Or just the gullibility of the fools sending their credit-card info to (account_deleted)@yahoo.com.

⚡ Biometrics technology: not yet ready for primetime

<"NewsScan" <newsscan@newsscan.com>>

Tue, 22 Jul 2003 09:27:32 -0700

Gartner Research director Anthony Allen told guests at the launch of European Biometrics Forum that while widespread use of biometrics was likely by 2008, the technologies still had some kinks to be ironed out. Biometrics, which includes technologies used for voice, face, iris and fingerprint identification systems, is virtually useless without adequate back security measures and databases, said Allen, and current systems have several fallibilities that must be corrected. For instance, evidence shows that wearing eyeglasses can fool an eyescanner, prosthetic makeup can confuse face scanners, a sore throat can change a voice print and breathing heavily on a fingerprint scanner can make prints unrecognizable. However, newer generations of technology are beginning to rectify some of these shortcomings; the latest fingerprint scanners now incorporate methods of detecting body heat and blood flow and can scan below the surface later, making it more difficult to deceive. [*The Register*, 22 Jul 2003; NewsScan Daily, 22 Jul 2003]

<http://www.theregister.co.uk/content/55/31865.html>

✶ Spammers who don't read RISKS

<<diamond@swcp.com>>

Sat, 26 Jul 2003 17:11:48 -0000

Reuters Internet Report:

A hoax e-mail was circulating around the Internet on Friday purporting to be a new cookery book from British celebrity chef Jamie Oliver dishing up recipes from sushi rolls to fish and chips.

Now here's the kicker:

Penguin Books, the UK publisher for Oliver's books, said it was trying to track down the e-mail's author. It contained a 121-page Microsoft Word document attachment replete with color photos, scores of recipes and a fictitious title, "The Naked Chef 2."

Anyone care to place bets on where they're most likely to find the author's name?

✶ Adieu to 'e-mail'?

<"NewsScan" <newsscan@newsscan.com>>

Mon, 21 Jul 2003 08:39:36 -0700

France's Culture Ministry has announced a ban on the use of the

word

"e-mail" in all government ministries, publications or Web sites and is encouraging French Internet users to adopt the term "courriel" when referring to electronic mail. Courriel is derived from "courrier electronique" -- electronic mail -- and, according to the General Commission on Terminology and Neology, the term is "broadly used in the press and competes advantageously with the borrowed 'mail' in English."

However, some Internet industry experts disagree with that assessment: "The word 'courriel' is not at all actively used. Protecting the language is normal, but e-mail's so assimilated now that no one thinks of it as American," says Marie-Christine Levet, president of French ISP Club Internet, who adds that her company has no plans to switch its terminology.

[AP, 19 Jul 2003; NewsScan Daily, 21 Jul 2003]

<http://apnews.excite.com/article/20030719/D7SCS9201.html>

[I presume this is in part the result of the use of the word "email"

(e'mail is a perfectly good French word relating to lacquer, and email

without the hyphen is unfortunately ACM's publication standard!). Nothing

in the foregoing to the contrary notwithstanding, my long-time crusade for

"e-mail" rather than "email" continues. See

<http://www.csl.sri.com/neumann/hyphen.html>

if you have not already. On the other hand, one of the musical instruments I play is certainly not a Freedom Horn. PGN]

✶ E-mail harvesting and re-use as a new virus vector?

<Jim Garrison <jhg@acm.org>>

Sat, 26 Jul 2003 21:34:31 -0500

I've recently received several e-mails from my Dad, with whom I regularly correspond. However, the subject lines and message texts were obviously not intended for me, and I was able to deduce both the intended recipient and the original time period when the messages were written, which was over a year ago. Each such message also contained an e-mail virus. The headers indicated the messages originated in Spain (where my Dad is living), but not from his ISP.

I think this represents a disturbing new trend in virus vectors, the 'harvesting' of messages and correspondence addresses in order to sneak in a virus disguised as a legitimate message from a trusted correspondent. I use Mozilla as my mail reader so of course I see the complete filename (file.doc.exe) and cannot be tricked into opening it, but people with Outlook or Outlook Express might easily be fooled.

Is this new, or have I just missed seeing it before? Anyone else having this experience?

[It's been around for some time, but seems to be increasing.
PGN]

Identity theft: a crime that pays?

<"NewsScan" <newsscan@newsscan.com>>

Tue, 22 Jul 2003 09:27:32 -0700

The number of victims that have fallen prey to identity thieves is severely underreported, according to a study by Gartner Research, which estimates that 3.4% of U.S. consumers -- about 7 million adults -- have suffered ID theft in the past year. Moreover, identity thieves generally get away with it -- arrests are made in only one out of every 700 cases. "The odds are really stacked against consumers," says Gartner VP Avivah Litan. "Unfortunately, they are the only ones with a vested interest in fixing the problem." Typically, victims of ID theft learn of the crime a year or more later after it happens -- long after the trail has gone cold. "It is different from payment fraud, where the thief takes a credit card number and consumers are innocent until proven guilty. With identity theft, it is the opposite: Consumers are thought to be guilty until proven innocent," says Litan. "There is a serious disconnect between the magnitude of identity theft that innocent consumers experience and the [financial] industry's proper recognition of the crime. Without external pressure from legislators and industry associations, financial services providers may not have sufficient incentive to stem the flow of identity crimes." [CNet News.com

21 Jul 2003; NewsScan Daily, 22 Jul 2003]

http://news.com.com/2100-1009_3-5050295.html

✶ Cross *words*?

<msb@vex.net (Mark Brader)>

Wed, 23 Jul 2003 10:57:03 -0400 (EDT)

I don't know how long it will remain online, but

<<http://www.guardian.co.uk/crossword/nonjava/blank/0,7095,-6003,00.html>>

currently contains a recent crossword puzzle from the British newspaper

The Guardian. And above the puzzle diagram, it says:

Special instructions: Two of the solutions to today's quick crossword

(no10362) contain numbers. Unfortunately, we cannot show numbers in

answers in the usual way. Click here to view a pdf file...

Risks of unwarranted character set assumptions!

[Pointed out by Owen McShane in rec.puzzles.crosswords.]

✶ Presidential "doublespeak" ...

<Jim Bauman <JBauman@safety-kleen.com>>

Thu, 24 Jul 2003 09:27:00 -0500

The risk here is that what is purported to be a way to enhance communication

could actually be a way to do the opposite (Hmmm ... Navigate nine Web pages

instead of sending an e-mail from your mail client to

president@whitehouse.gov ... Gee, which would you choose?). Is it a muddled

signal from the White House that they want the American public's feedback

and yet they don't?

Also, it's a handy way for the White House to sort its e-mail--- those in favor of their position and those who are not. Would then, the President or his people bother to read and consider the e-mails not favoring the White House's policy on a certain national/foreign affair? Would they pay more attention to those that favor their position?

Would they have an "accurate" number of e-mails in favor of their policies, but a nebulous one in regards to the e-mails that don't?

White House puts up obstacle course for e-mails

Critics cite burden of additional steps

By John Markoff, *The New York Times*, 18 Jul 2003

<http://www.chicagotribune.com/technology/chi-0307180184jul18,1,7186833.story>

Do you want to send an e-mail message to the White House? Good luck.

In the past, to tell President Bush--or at least those assigned to read

his mail--what was on your mind it was only necessary to sit down at a

personal computer connected to the Internet and dash off an e-mail note to

president@whitehouse.gov.

But this week, Tom Matzzie, an online organizer with the AFL-CIO, discovered

that communicating with the White House has become a bit more daunting. When

he sent an e-mail protest against a Bush administration policy, the message

was bounced back with an automated reply that instructed him to send the

message in a new way.

Under a system deployed on the White House Web site for the first time last

week, those who want to send a message to President Bush must navigate as many as nine Web pages and fill out a detailed form that starts by asking whether the message sender supports or differs with White House policy.

The White House says the new system, at <http://whitehouse.gov/webmail>, is an effort to be more responsive to the public and offer the administration "real-time" access to citizen comments. [...]

Owner of stolen 'sex.com' can sue VeriSign

<Monty Solomon <monty@roscom.com>>

Fri, 25 Jul 2003 23:04:16 -0400

Elinor Mills Abreu, Reuters, 25 Jul 2003

The owner of "sex.com," once considered one of the Internet's hottest addresses, can seek payment from the company that improperly transferred the domain to a "con man" who later fled to Mexico when ordered to pay \$65 million, a court ruled on Friday. The Ninth Circuit Court of Appeals in San Francisco ruled that "computer-geek-turned-entrepreneur" Gary Kremen can hold VeriSign Inc.'s Network Solutions unit liable for handing the sex.com Web address over to a "con man." The decision has widespread implications for companies that register domains, which until now have not been held responsible when Web sites are switched from their rightful owners, a lawyer

for the plaintiff said. ...

<http://finance.lycos.com/home/news/story.asp?story=35007290>

✶ Another risk of decency filters

<"J. Lasser" <jon@lasser.org>>

Sun, 20 Jul 2003 17:30:40 -0600

You could lose a customer.

I've moved out to Colorado and was pursuing broadband through my phone company. After they verified that my line was DSL-capable, they gave me a call and asked what ISP I'd like to use. Helpfully, they suggested that MSN had the best pricing deal with them.

After I agreed that this would be fine, they asked what user ID I would like. I said 'jonlasser' would be ideal. The system rejected that and several other variations due, the support technician decided, to the three-letter word buried in my last name. She asked if I'd like to pick another user ID.

I said no, and asked about other service providers I could use with their service. It turns out that there's an option for those of us who already have mail/web from elsewhere and just need the broadband, which is really what I wanted in the first place. But for that decency filter, however, MSN would have had another customer.

Jon Lasser jon@lasser.org 410-659-5333

✶ SCO wants licensing fees from corporate Linux users

<"monty solomon" <monty@roscom.com>>

Mon, 21 Jul 2003 17:48:44 -0400

SCO wants licensing fees from corporate Linux users
Otherwise, SCO said, companies could be in legal hot water
Todd R. Weiss, *Computerworld*, 21 Jul 2003

The gloves are now officially off -- all enterprise Linux users have to pay The SCO Group Inc. new licensing fees to use Linux, or they could find themselves on the wrong end of a copyright infringement lawsuit. That was the ultimatum laid out today by SCO CEO and President Darl McBride, who said that the \$3 billion lawsuit against IBM in March was apparently just the start of his company's march to defend itself from what it sees as rampant theft of its Unix System V intellectual property (IP). ...

<http://www.computerworld.com/softwaretopics/os/linux/story/0,10801,83287,00.html>

✶ Microsoft rediscovers MultiLevel Security

<Jeremy Epstein <jeremy.epstein@webmethods.com>>

Fri, 25 Jul 2003 14:01:31 -0700

Seems that Microsoft has rediscovered the value of MLS, allowing "analysts who hold the appropriate security clearance and have a need to know with the ability to access information across databases that may be compartmentalized or "air-gapped" for security reasons". The idea is to run multiple Oses on top of a VMWare (or similar) base, and then run multiple classifications of windows on the screen.

<http://www.computerworld.com/securitytopics/security/story/0,10801,83465,00.html?nas=PM-83465>

The more things change, the more they stay the same.

Re: Powergenitalia ([RISKS-22.81](#))

<Elijah Grabbet <eligrab@totalise.co.uk>>

Mon, 21 Jul 2003 16:09:37 +0100

It should be pointed out that while the unfortunately named <http://www.powergenitalia.com>

really exists, and it has caused much merriment in other newsgroups, too, it

is not the website of Powergen's [a British power company] Italian

subsidiary. As far as I know, Powergen does not even have an Italian subsidiary.

[This was noted by several RISKS readers. Many thanks. PGN]

⚡ Re: Error in E-Mini Dow Futures creates havoc at CBOT, CME

<Greg Compestine <gmc444@yahoo.com>>

Sat, 26 Jul 2003 17:07:49 -0600

> Apparently an order to sell 10,000 contracts instead of 100
> was put in by
> mistake.

Physical checking always uses double entry for amounts. Why not trading systems? Sounds like a perfect application for voice recognition technology (no pun intended). The person entering the number has to type in and then say the amount, and if the two don't agree, then the transaction isn't accepted.

⚡ Re: GPS-piloted tractors? (Heiney, [RISKS-22.81](#))

<Kent Borg <kentborg@borg.org>>

Mon, 21 Jul 2003 15:47:36 -0400

> The RISK of unmanned vehicles relying on GPS signals, with or without
> rotating blades attached, is interesting to contemplate, especially at night!

The article said nothing about "unmanned" tractors. This equipment is expensive, farmers aren't stupid, they don't send them off on their own, they ride in them.

Farmers also know that things that have nothing to do with GPS can go wrong

and they want to be there to notice and do something about them when they do.

Don't jump to such conclusions! If you want to worry about such things worry about unmanned lawn mowers or house vacuum cleaners or swimming pool vacuum cleaners even--they all do exist.

⚡ Re: GPS-piloted tractors? Hell yes! Que Stephen King!

<"Fredric L. Rice" <quack@skeptictank.org>>

Mon, 21 Jul 2003 11:24:42 -0700 (PDT)

In [RISKS-22.81](#) it's noted that there's advocacy of GPS-piloted tractors going into operation in Australia, sent in by Conrad Heiney who notes that tractors "with or without rotating blades attached is interesting to contemplate."

Where's the RISK? I *love* the idea of fully automated whirling machines of horrible, mangling death roaming the countryside at night, hiding from villagers by day, emerging in packs to assault gasoline stations to steal fuel, killing anyone who tries to stop them.

What's the down side? I'm sure Stephen King would agree with my delight that there are people out there working hard on the technology that would allow roaming packs of automated, economically efficient death to go from city to city harvesting and de-boning humans, cutting them into

manageable

sizes, and packaging them up in shrink wrap for your grocery shelf. Soylent

Green has to start somewhere!

These machines will dispassionately collect humans just as dispassionately

as they collect potatoes and I can't wait to see what hackers and anti-genetically modified food activists would make of such wonderful toys.

Man, I hope like hell they call the new technology "Godzilla."



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

[ACM](#) Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 83

Thursday 7 August 2003

Contents

- [Software violates stock ownership limits](#)
[Bill Hopkins](#)
- [Photoshop file contains more than the visible images](#)
[Nick Brown](#)
- [Virginia Identity Theft Passport](#)
[James Moyer](#)
- [Hand-held devices easy to hack](#)
[Monty Solomon](#)
- [What Time Is It?](#)
[Conrad Heiney](#)
- [Pentagon's online trading market plan draws fire](#)
[NewsScan](#)
- [New online futures market bets on next White House scandal](#)
[NewsScan](#)
- [Voting tech problems galore in Mississippi](#)
[Cathy Hayden via Kim Alexander](#)
- [Electronic voting - once again...](#)
[M Baumeister](#)
- [Why e-voting is a non-starter: Risks with e-voting](#)
[Bill Thompson via Chris Leeson](#)

- [Hospital records stuck in memory stick](#)
[Brett McCarron](#)
 - [Re: Domain names](#)
[Jay R. Ashworth](#)
[Sidney Markowitz](#)
[Paul Schreiber](#)
 - [Tech exodus: 500,000 U.S. jobs moving overseas](#)
[NewsScan](#)
 - [PFIR Forums Adds "Voting Systems" Discussion Group](#)
[Lauren Weinstein](#)
 - [REVIEW: "A Guide to Forensic Testimony", Fred Smith/Rebecca Bace](#)
[Rob Slade](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✂ **Software violates stock ownership limits**

<"Bill Hopkins" <whopkins@wmi.com>>

Mon, 4 Aug 2003 15:29:40 -0400

The New York Times reported Thursday that a Connecticut money manager inadvertently increased his holdings in two medical technology companies despite agreeing with both not to do so. He now owns 75% of one of the companies, whose CEO said he told them "three layers of software somehow failed" after he agreed in April to limit his investment at the 20% level. The other company went from 20% to 33%. Nobody noticed anything wrong until mid-July, despite steady buying.

The money manager is in apparent violation of SEC reporting requirements, which carry regulatory penalties. The companies face a protracted period of

uncertainty, as the positions are slowly unwound; one has a stock issue planned for this week. The institutional investors in the funds won't be able to unload it if the stock prices fall, and other investors in the companies who bought during the same period may wind up with losses if the stock prices prove to have been inflated.

For the money manager, some obvious RISKS :

- * Allowing computer software to run your business.
- * Layering software (no word, but I'll bet it's from different vendors).
- * Not sending the key memo to all three layers of software.
- * Checking your total holdings every three months.

For companies, the RISKS are less clear. It's not clear whether they had any way of finding out who was actually buying their stock, and that the price run-up was anything other than a general market recovery or recognition of value.

For investors, well, we all know NASDAQ is a crapshoot in the dark, don't we? (Big Julie will now remember where the spots used to be on the dice you just threw.)

The article, "Investor Says He Bought Stock and Didn't Know It," is at

<http://www.nytimes.com/2003/07/30/business/30PLAC.html>

(registration required, free access ends 8/06)

⚡ Photoshop file contains more than the visible images

<Nick Brown <Nick.BROWN@coe.int>>

Tue, 5 Aug 2003 20:45:02 +0200

A US TV presenter posted some artistic close-ups of her face. Using Photoshop before saving, she had apparently cropped pictures that were taken while she was posing topless. This enabled the crop to be undone.

This reminds us of what can happen in Word when you do a "regular" save. Apparently, Microsoft Word isn't the only application that stores more than what you see.

The subliminally-R-rated URL was previously on-line [http://www.shackspace.com/\[...\]](http://www.shackspace.com/[...]) but the link has been taken down, presumably due to heavy traffic from referrals from www.cruel.com.

[Recovering the hidden information must be known as a "cropshoot". PGN]

✶ Virginia Identity Theft Passport

<James Moyer <james@moyer.com>>
Mon, 04 Aug 2003 16:47:58 -0400

As part of my study of photo ID documents (and the theory for explaining how they work, the current version of my paper is at <http://www.njlicense.org/sdt.pdf>), I've been trying to figure out the trust failure portion of Security Document Theory.

Trust failure occurs when a document is no longer believed to be valid. Too much counterfeiting or other security problems causes too many

bad documents

to be in the wild, though I believe that institutions can turn their backs on ID documents, which sometimes occurs in countries that have national ID cards. (People from several different countries, such as Italy and Argentina, have told me that police may just decide not to trust their ID card, and haul them in to get their identity assessed differently.)

The Virginia Identity Theft Passport is a different variation of that. The trust has eroded from the normal documents, and now people, in certain situations, need yet another document to back up their current assortment of documents. (My theory considers photo ID card trust failures inevitable, as long as the photo ID card performs multiple functions which have value to criminals.)

I'm particularly amused by the reductio ab absurdum for the theft passport. Instead of a separate document, why couldn't it be an endorsement on the individual's driver's license (which would imply something like "this is a regular John Smith, who is not *that* John Smith." Or "this is a *real* Virginia driver's license."

⚡ Hand-held devices easy to hack

<Monty Solomon <monty@roscom.com>>

Sun, 3 Aug 2003 00:37:49 -0400

Hand-held computers used to store phone numbers, medical and credit-card information leave millions of gadget lovers fully exposed to identity-theft and other crimes, security experts said on Saturday. Software is now widely available to allow people to steal passwords and other information from popular Palm-based computers, especially when they connect to other computers to share data, said Bryan Glancey, a manager at wireless security services provider MobileArmor of St. Louis, Missouri. While millions of people now rely on handy electronic scheduling and address books, few carry sufficient security protections to prevent identity theft if the hand-held is lost or stolen, as is commonplace. Simple programs exist to uncover even hidden data, Glancey said. Other software allows people to steal data while remaining at some distance from the victims, he added. ...

[Source:

Reuters, 2 Aug 2003]

<http://finance.lycos.com/home/news/story.asp?story=35114601>

What Time Is It?

<"Conrad Heiney" <conrad@fringehead.org>>

Mon, 4 Aug 2003 12:47:15 -0700

The Guardian has a fascinating story on the ITU's Study group concerned with time. According to the article, divergent time systems are an increasing problem. Conflicts between Earth time, the time provided by

atomic clocks, GPS time, and other standards raise interesting questions about the safety of aircraft and other complex systems that may be running on different timescales.

http://www.guardian.co.uk/uk_news/story/0,3604,985020,00.html

✶ Pentagon's online trading market plan draws fire

<"NewsScan" <newsscan@newsscan.com>>

Tue, 29 Jul 2003 09:23:30 -0700

The U.S. Defense Department's Defense Advanced Research Projects Agency (DARPA) has plans to set up an online Policy Analysis Market that will allow traders to bet on the likelihood of future terrorist attacks and political assassinations in the Middle East. The bizarre scheme has drawn fire from Senators Ron Wyden (D-Ore.) and Byron Dorgan (D-N.D.). "The idea of a federal betting parlor on atrocities and terrorism is ridiculous and it's grotesque," said Wyden, while Dorgan described the plan as "useless, offensive and unbelievably stupid. How would you feel if you were the King of Jordan and you learned that the U.S. Defense Department was taking bets on your being overthrown within a year?" However, the Pentagon defended the initiative, comparing it to commodity futures markets. "Research indicates that markets are extremely efficient, effective and timely aggregators of dispersed and even hidden information. Futures markets have proven

themselves to be good at predicting such things as election results; they are often better than expert opinions." The market would allow traders to deposit money in an account and then use it to buy and sell contracts. If a particular event comes to pass, the bettors who wagered correctly would win the money of those who guessed wrong. [BBC News 29 Jul 2003; NewsScan Daily, 29 Jul 2003]

<http://news.bbc.co.uk/1/hi/world/americas/3106559.stm>

[This plan was subsequently scrapped. One of its proponents, John Poindexter (head of DARPA's IAO office), reportedly will be retiring.

PGN]

✶ New online futures market bets on next White House scandal

<"NewsScan" <newsscan@newsscan.com>>
Mon, 04 Aug 2003 10:58:36 -0700

In response to the Pentagon's now-discarded plans for a terrorism futures market, academics from half a dozen U.S. universities have created an American Action Market, which will offer traders the opportunity to wager on the likelihood of various Washington political events, such as: Which country will the White House threaten next? Who will be the next foreign leader to move off the CIA payroll and onto the White House's "most wanted" list? Which corporation with close ties to the White House will be the next

cloaked in scandal? The AAM will begin registering traders in September and will open for business October 1. "It's quite amazing, the Pentagon and the White House are very fertile imaginative fields these days," says one of the AAM founders. "(The AAM project) sounds humorous, but that just shows how far things have gone. We've entered the realm of fiction. Things are really Dr. Strangelove." Bob Forsythe, a University of Iowa professor who helped set up the Iowa Electronic Markets that speculate on election results, says such futures markets can deliver fairly accurate predictions, but the traders have to be knowledgeable. "You have to have informed traders or they don't work very well. Who are the informed traders in an assassination market, for example? The same is true for predicting the White House."

[Wired.com 4 Aug 2003; NewsScan Daily, 4 Aug 2003]

<http://www.wired.com/news/politics/0,1283,59879,00.html>

✶ Voting tech problems galore in Mississippi

<Kim Alexander <kimalex@calvoter.org>>

Wed, 6 Aug 2003 11:59:43 -0700

Errors - human, mechanical - mar Election Day

By Cathy Hayden, chayden@clarionledger.com [PGN-ed]

<http://www.clarionledger.com/news/0308/06/melec02.html>

Election officials and political party offices were flooded all day on 5 Aug

2003 with reports of voting snafus ranging from locked precincts to machine

malfunctions to voters receiving ballots with the wrong names on them.

"It's worse than it has been in 10 years," said Claude McInnis, chairman of the Hinds County Democratic Party. "We had redistricting.

That made it much more complex." [...]

Because Mississippi has 82 counties and there are party primaries, "164 groups of people are running the elections - the Republican county executive committee in every county and Democratic county executive committee. There's a lot happening," according to David Blount, spokesman for Secretary of State Eric Clark.

[The article quotes a voter who did not recognize anyone on the ballot --

he had been given the wrong ballot, probably the fault of the poll worker.

Usual tales of a precinct that was locked for three hours (with poll workers

operating out of their own vehicles), nonworking touch-screen systems,

failure to read the initialization chip, etc. PGN]

Kim Alexander, President, California Voter Foundation

kimalex@calvoter.org, 916-441-2494, <http://www.calvoter.org>

⚡ Electronic voting - once again...

<M Baumeister <MBAUMEISTR@aol.com>>

Thu, 24 Jul 2003 18:32:47 EDT

"According to election industry officials, electronic voting systems are absolutely secure, because they are protected by passwords and

tamperproof
audit logs. But the passwords can easily be bypassed, and in fact the audit logs can be altered. Worse, the votes can be changed without anyone knowing, even the County Election Supervisor who runs the election system."

... for the rest of the story:

Inside A U.S. Election Vote Counting Program [by Bev Harris]
<http://www.scoop.co.nz/mason/stories/HL0307/S00065.htm>

✶ Why e-voting is a non-starter: Risks with e-voting

<"LEESON, Chris" <CHRIS.LEESON@london.sema.slb.com>>

Mon, 28 Jul 2003 10:20:38 +0100

Bill Thompson has written an article on the BBC Website about the Risks of Electronic Voting:

<http://news.bbc.co.uk/1/hi/technology/3095705.stm>

He starts by mentioning the recently-revealed DirectX flaw, security problems in Windows Server 2003, and thefts from a South African bank due to e-mail sniffing.

He then mentions the general problems with Authentication, and then some specific problems found with the Diebold Election Systems equipment. He caps this section of the article with noting that the company concerned refuses to allow independent code reviews on the grounds of commercial confidentiality.

In other words, the same old story.

The article closes with the following paragraphs:

The British Government is still set on giving us all easy ways to vote,
and the pilots from last year's council elections are being extended.

There is still talk of online voting in the next general election, and of
moving away from paper ballots entirely in the future.

Yet every time we get to look inside a piece of software or a security
system that has been developed in secret, and built on the top
of a
compromise between acceptable levels of risk and the cost of
doing it
properly, we find holes and errors.

This is the reason why we must not move to an online voting
system. It
cannot be made secure, it cannot be guaranteed and it cannot
be trusted,
no matter who writes it, and no matter what claims are made.

A democratically elected government of the United Kingdom has
massive
power. The gains to be made from undermining a general
election are just
too high for us to take the risk of moving the election online.

Paper ballots and physical presence in the polling station
make the system
too unwieldy to hack. We should keep it that way.

✶ Hospital records stuck in memory stick

<"Brett McCarron" <MCCARBWM@dfw.wa.gov>>

Thu, 07 Aug 2003 08:59:54 -0700

Hospital bosses in Greater Manchester have tightened up IT security procedures after a Crewe estate agent found a memory stick sold as new contained confidential details of 13 cancer patients.

A report into the security breach, which happened earlier this year, found that the data had been transferred onto the memory stick when a computer storing a database of patient details was sent for an upgrade. The hospital's IT supplier Pocos took the computer to MBS Computers in Crewe, where the data was copied onto the stick. But the investigation was unable to ascertain how it then came to be sold as new.

<http://silicon.com/news/500013-500001/1/5491.html>

http://zdnet.com.com/2110-1105_2-5060979.html

[I'll bet that opened package memory sticks sell pretty quickly at computer superstores - BWM].

Brett McCarron, IT Security & Policy Officer, WDFW Information Technology Services, 600 Capitol Way N. - Olympia, WA 98501-1091 (360) 902-2331

✶ Re: Domain names ([RISKS-22.81](#))

<"Jay R. Ashworth" <jra@baylink.com>>
Mon, 4 Aug 2003 12:45:04 -0400

Darryl Luff apparently reads Dave Barry's weblog. :-)
So do I, but as far as I know, Dave got the other one from me:

<http://www.whorepresents.com>

Isn't it nice that DNS is case-insensitive so that you can use WhoRepresents.com instead?

Jay R. Ashworth, Member of the Technical Staff, Baylink, The Suncoast Freenet
Tampa Bay, Florida jra@baylink.com <http://baylink.pitas.com> +1
727 647 1274

⚡ Re: Domain Names ([RISKS-22.81-82](#))

<Sidney Markowitz <sidney@sidney.com>>

Mon, 28 Jul 2003 12:04:34 +1200

[RISKS-22.82](#) correctly points out that powergenitalia.com is not the Web site of some Italian subsidiary of the British firm Powergen, and the Web site today (as I type this) is just an "under construction" page. HOWEVER, there was a company Web site there when it was mentioned in [RISKS-22.81](#). You can *try* to hide, but often not successfully on the Web. The Internet Wayback Machine reveals that there is a company named Powergen Italia (or else a very longstanding Web hoax). Their location and history can be found at:

<http://web.archive.org/web/>

[20020210171927/www.powergenitalia.com/inglese/logol.htm](http://web.archive.org/web/20020210171927/www.powergenitalia.com/inglese/logol.htm)

<http://web.archive.org/web/>

[20020203231738/www.powergenitalia.com/inglese/aziendae.html](http://web.archive.org/web/20020203231738/www.powergenitalia.com/inglese/aziendae.html)

The whois information matches the information there:

<http://opensrs.org/cgi-bin/whois.cgi?action=lookup&domain=powergenitalia.com>

⚡ Re: Domain Names ([RISKS-22.81-82](#))

<Paul Schreiber <shrub@mac.com>>

Tue, 29 Jul 2003 18:26:35 -0400

I've seen this before: the dotcom "experts exchange" had the domain expertsexchange.com ... ExpertSexChange.com? Ooops!

[Ah, another item for my Hyphen(h)ater's Handbook? PGN]

⚡ Tech exodus: 500,000 U.S. jobs moving overseas

<"NewsScan" <newsscan@newsscan.com>>

Wed, 30 Jul 2003 09:36:42 -0700

One out of 10 jobs in the U.S. computer services and software sector could move overseas by the end of next year, according to a new report from Gartner Inc. And while professionals in the computer industry will be especially hard-hit, IT jobs in other sectors such as banking, health-care and insurance will feel the impact also, with one in 20 being exported to emerging markets such as Russia, India or other countries in Southeast Asia. "Suddenly we have a profession -- computer programming -- that has to wake up and consider what value it really has to offer," says Gartner VP and research director Diane Morello. Morello estimates that based

on her preliminary calculations, at least 500,000 jobs will be lost to offshore outsourcing by then end of 2004. The trend toward "offshore outsourcing" is heating up as a political issue, with legislators in five states proposing bills that would require workers hired under state contracts be American citizens or fill a special niche that citizens cannot. [Reuters/CNN.com 30

Jul 2003; NewsScan Daily, 30 July 2003]

<http://www.cnn.com/2003/TECH/internet/07/30/jobs.oversees.reut/index.html>

✶ PFIR Forums Adds "Voting Systems" Discussion Group

<pfir@pfir.org (PFIR - People For Internet Responsibility)>

Wed, 6 Aug 2003 11:59:26 PDT

PFIR - People For Internet Responsibility - <http://www.pfir.org>

The PFIR Forums discussion board located at:

<http://forums.pfir.org>

has added a new discussion group topic:

"Voting Systems - Benefits and Risks"

for the discussion of the benefits, risks, problems and solutions related to voting technologies, including mechanical and electronic (e-voting) systems, especially optical scan, computer-based, and Internet voting. This group is moderated by Peter G. Neumann.

Other discussion groups (all are moderated) on PFIR Forums include:

Civil Liberties vs. Technology

Advanced and useful technologies are becoming massive threats to privacy and other civil liberties. How can technology be appropriately controlled and civil liberties protected?

E-Mail Issues, Problems, and Solutions

Discussion of problems, possible solutions, and a wide range of other issues relating to e-mail, including PFIR's Tripoli e-mail proposal

Informational (read-only) groups include:

Fact Squad Radio

Recent listings and e-mail notification for PFIR's Fact Squad Radio short mp3 audio features

PFIR Forums Information and Guidelines

Basic information, usage guidelines, privacy policy, etc. for PFIR Forums

As always, your participation in PFIR Forums is cordially invited.

Thank you very much.

Lauren Weinstein <http://www.pfir.org/lauren>

lauren@pfir.org lauren@vortex.com lauren@privacyforum.org +1-818-225-2800

Co-Founder, PFIR - People For Internet Responsibility - <http://www.pfir.org>

Moderator, PRIVACY Forum - <http://www.vortex.com>

⚡ REVIEW: "A Guide to Forensic Testimony", Fred Smith/ Rebecca Bace

<Rob Slade <rslade@sprint.ca>>

Tue, 29 Jul 2003 10:54:51 -0800

BKGFOTS.RVW 20030604

"A Guide to Forensic Testimony", Fred Chris Smith/Rebecca Gurley Bace,
2003, 0-201-75279-4, U\$49.99/C\$77.99
%A Fred Chris Smith
%A Rebecca Gurley Bace
%C P.O. Box 520, 26 Prince Andrew Place, Don Mills, Ontario
M3C 2T8
%D 2003
%G 0-201-75279-4
%I Addison-Wesley Publishing Co.
%O U\$49.99/C\$77.99 416-447-5101 fax: 416-443-0948 bkexpress@aw.com
%O [http://www.amazon.com/exec/obidos/ASIN/0201752794/
robsladesinterne](http://www.amazon.com/exec/obidos/ASIN/0201752794/robsladesinterne)
[http://www.amazon.co.uk/exec/obidos/ASIN/0201752794/
robsladesinte-21](http://www.amazon.co.uk/exec/obidos/ASIN/0201752794/robsladesinte-21)
%O [http://www.amazon.ca/exec/obidos/ASIN/0201752794/
robsladesin03-20](http://www.amazon.ca/exec/obidos/ASIN/0201752794/robsladesin03-20)
%P 509 p.
%T "A Guide to Forensic Testimony"

The subtitle explains the book more fully: "The Art and Practice of Presenting Testimony as an Expert Technical Witness." However, those with expectations about the form of technical literature should note that the style of this work follows that of the legal profession and case law: it primarily teaches by using examples rather than pointing out a specific methodology.

The preface illustrates another difference between the technical and legal worlds. Computer work generally involves finding an answer to a problem: if the code works, background study and documented analysis is generally irrelevant. The legal profession, on the other

hand,
absolutely depends upon advance preparation, and an answer is almost
useless unless the reasoning, background, and process is not only
chronicled, but properly and legally obtained. Thus the authors
are
aware of the twin needs to inform technical experts about the
requirements of the legal world, and to instruct legal
professionals
in aspects of technology that may be relevant to the pursuit of a
case. The introduction notes the possible tragedies that can
result
if either the trial attorney or the technical expert attempts to
act
as ventriloquist to the other's dummy.

Chapter one gives examples of expert witnesses, starting with a
fictional example from a movie. Normally this would not be very
instructive, but the authors are careful to point out, from the
fictional story, important legal points to be aware of in regard
to
the possibilities and limits of expert testimony (and also the
legal
restrictions that would prevent some of the story points from
happening in a real case). The rest of the chapter then goes on
to
introduce legitimate and recognized experts, and present their
opinions and advice in regard to the practice of expert
testimony.

Chapter two is supposed to promote both the idea of becoming an
expert
witness, and of preparing for the experience. In fact, most of
the
material deals with Bill Gates' first deposition in the antitrust
litigation, and the mistakes that he made. The example does make
valid points both about the value of preparation and the need to
testify whether we want to or not, but the message is not always
obvious. Using testimony to provide a story about what happened
is
presented in chapter three. The example, though, is the tracing
of
Kevin Mitnick's intrusion on the systems managed by Tsutomu
Shimomura,

and therefore the testimony, which never happened, is simulated, which weakens the lessons the text intends to convey. Chapter four outlines the rules of testimony and the legal process, and is the section that technical people should probably study most thoroughly. Although there are important points to be made in regard to the dangers of reasoning beyond the facts, chapter five reads more like an editorial inveighing against pseudoscience.

Ethical issues are discussed in chapter six. The early material involves a great deal of text from two case decisions, but eventually there is a review of codes of conduct, and even examination of some of the moral aspects of court battles. Chapter seven deals specifically with the matter of bias. The gatekeeper function of American judges, who must decide not only whether a witness is truly expert, but on what the expert may testify about or to, is covered in chapter eight. This material also reviews important points about the qualifications for experts and the characteristics of good evidence. Credible and convincing evidence and presentation is described in chapter nine, and this is extended to visual exhibits in chapter ten, demeanour in eleven, and non-verbal communications in twelve. Chapter thirteen contains examples of, and advice from, some experts who have extensive experience in court testimony.

The book sometimes flows rather oddly, and it would be easy to take issue with a number of the topics or the emphasis given to certain ones over others. Even so, this work *is* important, and

information

security professionals; and certainly those in management or consulting roles; should seriously consider it. The text is written

with the technical worker in mind, although legal professionals would

undoubtedly find the research, advice, and explanations to be helpful

in preparing for technical cases. Litigation involving technical topics is increasing all the time, and new (and therefore unfamiliar)

technologies are now as constant a fact of legal life as forensic concerns are in technical work.

copyright Robert M. Slade, 2003 BKGDFOTS.RVW 20030604
rslade@vcn.bc.ca slade@victoria.tc.ca rslade@sun.soci.
niu.edu

<http://victoria.tc.ca/techrev> or <http://sun.soci.niu.edu/~rslade>



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

[ACM](#) Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 84

Monday 11 August 2003

Contents

- [Identity Crisis, article by Robert O'Harrow Jr.](#)
[PGN](#)
- [Man proves he was victimized by network vandals](#)
[NewsScan](#)
- [Dutch price index wrong due to software error](#)
[Erling Kristiansen](#)
- [Worker deletes herself out of job](#)
[M Taylor](#)
- [UCITA support fading fast](#)
[NewsScan](#)
- [Judge throws out RIAA subpoenas](#)
[NewsScan](#)
- [Who profits from spam? Surprise!](#)
[Bob Sullivan via Monty Solomon](#)
- [Ticketmaster privacy policy slammed](#)
[Paul Festa via Monty Solomon](#)
- [Hacker gets Acxiom customer information](#)
[Caryn Rousseau via Monty Solomon](#)
- [Acxiom's FTP Server compromised by /now former/ client](#)
[Randy Holcomb](#)

- [Software patching gets automated](#)
[William Jackson via Lillie Coney](#)
 - [How many Windows crashes occur in a year?](#)
[John Dvorak via Monty Solomon](#)
 - [Company's error sends customers to Massachusetts adult phone line](#)
[Monty Solomon](#)
 - [University library catalogue + security](#)
[Richard A. O'Keefe](#)
 - [GenCon Registration Woes Blamed on Computer Network](#)
[Allan Goodall](#)
 - [Re: Metadata in Photoshop files](#)
[Sidney Markowitz](#)
 - [Re: New online futures market bets on next White House scandal](#)
[Stephen R. Holmes](#)
 - [Re: Software violates stock ownership limits](#)
[John R. Levine](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ Identity Crisis, article by Robert O'Harrow Jr.

<"Peter G. Neumann" <neumann@csl.sri.com>>

Sat, 9 Aug 2003 11:33:27 PDT

The Washington Post Magazine Cover Story:

Identity Crisis, by Robert O'Harrow Jr.

<http://www.washingtonpost.com/wp-dyn/articles/A25358-2003Aug6.html>

Caption on pair of photos:

LEFT:

Meet Michael Berry: political activist, cancer survivor, creditor's dream.

RIGHT:

Meet Michael Berry: scam artist, killer, the real Michael Berry's worst nightmare ...

[This is an extraordinary article. MUST READING for all of us victims-in-waiting. PLEASE dig it out while it is still on-line. PGN]

⚡ Man proves he was victimized by network vandals

<"NewsScan" <newsscan@newsscan.com>>

Mon, 11 Aug 2003 09:16:20 -0700

In the U.K., a man has been acquitted in Exeter Crown Court after successfully arguing that child pornography found on his personal computer had been placed there without his knowledge by network vandals who had used a "Trojan horse" program to infect his machine. The case creates two worries: one, that actual child pornographers now have a new alibi that would be difficult to disprove; two, that innocent Web surfers might find themselves charged with possessing illegal material planted on their computers by malicious invaders. Former U.S. federal computer crime prosecutor Mark Rasch says, "The scary thing is not that the defense might work. The scary thing is that the defense might be right. The nightmare scenario is somebody might go to jail for something he didn't do because he was set up." [*The New York Times*, 11 Aug 2003; NewsScan Daily, 11 Aug 2003] <http://partners.nytimes.com/2003/08/11/technology/11PORN.html>

⚡ Dutch price index wrong due to software error

<Erling Kristiansen <erling.kristiansen@xs4all.nl>>

Thu, 07 Aug 2003 22:13:23 +0200

The Dutch Central Bureau of Statistics (CBS) published an incorrect price index due to "an error in a computer program", according to the newspaper Trouw (7 August). The published index was too high by "a few tenths of a percent". No further explanation is given as to the nature of the error, why it was not discovered before publication, or how it was discovered later.

This may have an impact on salary adjustments as well as pensions and various social benefits that are linked to the inflation rate.

This is yet another example of how dependent we have become on "the computer says so, so it must be right". A few tenths of a percent on a country-wide basis, even in a small country, adds up to a lot of money.

⚡ Worker deletes herself out of job

<M Taylor <mctaylor@privacy.nb.ca>>

Thu, 7 Aug 2003 21:31:17 +0100

A Nova Scotia [Canada] government employee has been fired for deleting her own speeding ticket from a computer database. ... The unidentified woman will not face criminal charges.

Now the kicker is she was found by an audit conducted after another employee had also altered entries in the database of driver's records. Why can people delete records from such a database? Shouldn't it operate like the accountant's double-entry ledger? Where mistakes are not deleted, but a correction entry is appended.

http://novascotia.cbc.ca/regional/servlet/View?filename=ns_firedwork20030806

M Taylor <http://www.mctaylor.com/>

UCITA support fading fast

<"NewsScan" <newsscan@newsscan.com>>
Fri, 08 Aug 2003 11:08:16 -0700

Key backers of the Uniform Computer Information Transactions Act (UCITA) have bowed to pressure from opposition groups and will stop lobbying for the bill's passage. The bill was intended to protect software developers from intellectual property theft by bringing into conformity conflicting software licensing laws in various states, but critics, including the American Bar Association and the American Library Association, said the legislation would grant software makers too much power over their products at the expense of consumers. So far, UCITA has been enacted in only two states, Maryland and Virginia, and now that the effort has lost the support of the National

Conference of Commissioners on Uniform State Laws (NCCUSL), UCITA is unlikely to gain further consideration from other states, says an NCCUSL spokeswoman. Opponents of the bill commended NCCUSL for its decision: "It is heartening to see NCCUSL backing away from a very flawed statute, but it will never be able to write sound law for the information economy until it takes to heart the criticisms of the user sector," said Jean Braucher, a law professor at the University of Arizona and a member of AFFECT -- Americans For Fair Electronic Commerce Transactions. [CNet News.com 7 Aug 2003; NewsScan Daily, 8 August 2003]

http://news.com.com/2100-1028_3-5061061.html?tag=fd_top

⚡ Judge throws out RIAA subpoenas

<"NewsScan" <newsscan@newsscan.com>>

Mon, 11 Aug 2003 09:16:20 -0700

A federal judge in Boston has rejected subpoenas filed by the Recording Industry Association of America last month as part of its nationwide crackdown on digital music file-sharing. The subpoenas targeted students at Boston College and the Massachusetts Institute of Technology who used various screen names to share songs online. In his ruling, Judge Joseph L. Tauro said that under federal rules, subpoenas issued in Washington cannot be served in Massachusetts. The RIAA called the ruling "a minor

procedural

issue" but declined to say whether it would refile in Boston.

pAP 8 Aug

2003; NewsScan Daily, 11 Aug 2003]

<http://apnews.excite.com/article/20030809/D7SQ5LC80.html>

Who profits from spam? Surprise! (Bob Sullivan)

<Monty Solomon <monty@roscom.com>>

Sun, 10 Aug 2003 12:27:27 -0400

Many companies with names you know are benefiting

Bob Sullivan, MSNBC, 8 Aug 2003

There wouldn't be spam if there wasn't money in spam. So to understand what

primes the spam economy, MSNBC.com answered a single unsolicited commercial

e-mail. Following this one spam trail led us from Alabama to Argentina, from

a tiny Birmingham-based firm and someone named "Erp" past a notorious

spammer named Super-Zonda - and right through big-name companies like

Ameriquist, Quicken, and LoanWeb. And that's just the beginning.

The truth

about spam is this: While the dirty work is done by secretive, faceless

computer jockeys who are constantly evading authorities, lots of companies

with names you know profit, at least tangentially, from their efforts. ...

<http://www.msnbc.com/news/940490.asp>

Ticketmaster privacy policy slammed (Paul Festa)

<Monty Solomon <monty@roscom.com>>

Fri, 8 Aug 2003 01:30:04 -0400

By Paul Festa, CNET News.com, 6 Aug 2003

People buying tickets online through Ticketmaster may be surprised to find themselves receiving spam as an encore. The ticket service, which holds a lock on advance ticket sales for most major entertainment events, is taking heat from consumers for a privacy policy that does not let online ticket buyers opt out of receiving e-mail pitches from an event's producers and other businesses associated with it. That, Ticketmaster critics say, means that the company has made receiving spam part of the price of admission.

"I have only bought a single ticket from Ticketmaster, many years ago," wrote one customer on an online discussion board devoted to the privacy policy. "Since that purchase, I have received tons of 'targeted' e-mail personalized with my full name, the city, etc...For now, I do everything I can to avoid ticket purchases from Ticketmaster (and have been successful)."

The Ticketmaster privacy policy under fire states that customers may "opt out" of getting e-mail from Ticketmaster itself, but cannot refuse to share their personal information with "event partners" -- defined as "the venues, promoters, artists, teams, leagues and other third parties associated with that concert, game or other event." ...

<http://news.com.com/2100-1026-5060827.html>

⚡ Hacker gets Acxiom customer information (Caryn Rousseau)

<Monty Solomon <monty@roscom.com>>

Fri, 8 Aug 2003 02:20:18 -0400

By Caryn Rousseau, Associated Press, 7 Aug 2003

A computer hacker gained access to private files at Acxiom Corp., one of the world's largest consumer database companies, and was able to download sensitive information about some customers of the company's clients, the company said Thursday. "The data on the servers was a wide variety of information, some of which was personal, some of which was not," Jennifer Barrett, the company's chief privacy officer, said in an interview with The Associated Press on Thursday. The AP was notified of the intrusion by an anonymous caller who would not identify himself or his connection with the company. Barrett said the company did not know about the breach until a law enforcement agency from Ohio contacted it last week. Barrett said both the hacker and the stolen information are in police custody. She said about 10 percent of the company's customers were affected and that, "it would include some of our larger customers." ...

<http://finance.lycos.com/home/news/story.asp?story=35190673>

⚡ Acxiom's FTP Server compromised by /now former/ client

<"Randy Holcomb" <rholcomb@speakeasy.net>>

Fri, 8 Aug 2003 21:31:18 -0500

"... The breach involved one external FTP server outside Acxiom's firewall that is used to transfer files back and forth between Acxiom and its clients. The company said no internal databases were accessed and no breach penetrated its firewall. Additionally, the firm said only a small percentage of its clients' data was involved in the incident.

Acxiom's client list includes a number of Fortune 500 companies, like Microsoft, IBM, AT&T, and Blockbuster. The company says it services 14 of the top 15 credit card companies, 7 of the top 10 auto makers, 7 of the top 10 media entertainment companies, 6 of the top 10 magazine publishing companies, 4 of the top 5 telecom companies, 5 of the top 6 retail banks and 3 of the top 5 retailers. ..."

<http://www.internetnews.com/article.php/2246461>>

⚡ Software patching gets automated (William Jackson)

<Lillie Coney <lillie.coney@acm.org>>

Fri, 08 Aug 2003 15:09:26 -0400

By William Jackson, GCN Staff

Whenever the Defense Department's Computer Emergency Response Team

Coordination Center sends out a vulnerability alert, each DoD systems administrator must acknowledge it and respond with a plan for closing the hole. The notification and response is becoming more automated, said a security manager at a DoD software development shop, who contacted GCN and asked that neither he nor his agency be named in print. The problem is that the remediation is manual. When you get two or three alerts an hour, it gets out of control. The DoD security manager said he uses the Hercules automated remediation tool from Citadel Security Software Inc. of Dallas to cut the time for fixing flaws in multiple machines from weeks to days or hours. [...]

[And when it is **fully** automated, think of how wonderful it will be to have new Trojan horses and security flaws installed instantaneously, without having to require human intervention. Perhaps someday we might have systems that do not require continual patching, but I'm not holding my breath. PGN]

⚡ How many Windows crashes occur in a year? (John C. Dvorak)

<Monty Solomon <monty@roscom.com>>
Sat, 9 Aug 2003 00:26:44 -0400

Magic Number: 30 Billion
By John C. Dvorak, 4 Aug 2003

So what actually happens when your Windows XP machine crashes

and asks if you want to send a report? The reports obviously accumulate in some database, and I can only assume that when one bin piles up with similar crash memos, the coders get to work. Exactly how many notifications does Microsoft get? Nobody knows for sure, but based on comments Bill Gates made at a recent meeting for analysts, the number must be astronomical.

Gates said that 5 percent of Windows machines crash, on average, twice daily. Put another way, this means that 10 percent of Windows machines crash every day, or any given machine will crash about three times a month. Since Bill is a math junkie, I have to assume this number is real and based on something other than a phone survey. Those reports seem like the obvious source.

Now according to StatMarket.com, as of March 2003, Windows XP had 33.41 percent global market share among operating systems. Let's give Microsoft the benefit of the doubt and make Windows XP's share an even 35 percent at this point. How many computers are in use? According to the Computer Industry Almanac, there were 603 million worldwide in 2001, and the growth rate seems to be around 10 to 15 percent per year. Let's be relatively conservative, and add just under 100 million to get a round number of 700 million PCs. With 10 percent of them crashing daily, we have 70 million crashes every 24 hours. And since only 35 percent are XP machines, 24.5 million reports a day accumulate in Redmond-nearly 9 billion per

year. I

doubt this number will go down anytime soon. ...

<http://www.pcmag.com/article2/0,4149,1210067,00.asp>

[Wonderful article. John goes on to estimate that this works out to a

minimum of 30 billion Windows system crashes per year. He points out that

this magic number is also the number of gallons of fresh water California

wastes because of mismanagement, the dollar total for the Enron scam, and

a few other nice examples. But he concludes that he is partial to the

number ZERO, and thinks maybe that should be the target for Microsoft.

PGN]

✶ Company's error sends customers to Massachusetts adult phone line

<Monty Solomon <monty@roscom.com>>

Fri, 8 Aug 2003 01:01:44 -0400

Associated Press, 6 Aug 2003

Some unsuspecting Verizon customers trying to pick a new long-distance plan

were offered ''sexy introductions'' and a chance to ''continue the fun'' on

an adult phone line. A letter sent to thousands of Verizon long-distance

customers across the country last week listed a number for ''Intimate

Connections'' as a Verizon customer service number, Verizon officials said

Tuesday. ...

<http://www.boston.com/dailynews/218/region/>

[Company_s_error_sends_customer:.shtml](#)

✶ University library catalogue + security

<"Dr Richard A. O'Keefe" <ok@cs.otago.ac.nz>>

Mon, 11 Aug 2003 15:25:32 +1200

Until recently, our university library used a DYNIX catalogue. That had a Telnet interface and a Web interface; I always used the Telnet interface because that way I could get things done quicker.

We now have a new catalogue, called Conzulsys, which you may be able

to view at <https://otago.conzulsys.ac.nz>.

It's described as the "New Zealand Universities' Shared Library System",

and indeed one can look up things in (a few) other libraries as well.

Problems.

(1) There isn't a Telnet interface any more. This means that I can no

longer use 'expect' to drive queries. Chizz.

(2) The interface isn't really designed for any of the machines I use (a

SunBlade100 and a G3 PowerMac). For example, quite a lot of buttons

have black text on a dark blue background, so that I cannot see what

the buttons actually are. The navigation links at the top of the page

are images, even though they are just plain text, and they're a little

too small to read comfortably on a 90dpi screen.

(3) The ***** thing keeps timing out. For example, just now I started a

multisite search for a particular author; it popped up a

window showing

me that the searches had started, and then a second later, before

delivering any results, said "Restart Web Voyage Your Catalogue session timed out due to inactivity." How can that be

when I've just entered a query? And now that's happened, it doesn't

matter what I click, I get the same stupid timeout page.

(4) When new books come into the library, they are put on a rack of

"New Arrivals" shelves. It used to be that you could take them over

to a terminal and book them. Now you have to fill out a paper form and

hand it to the librarians, and at the end of the week they have to spend

several hours sorting these things out by hand. (Literally sorting to

get priority right; you have to fill out the time you put the form in.)

(5) You might not have predicted (3) or (4), but you probably *could* have

predicted this one. The HTML they generate is systematically bad.

A <LINK> element is used to connect a page to its style sheet, BUT

it is put in the <BODY> instead of the <HEAD> where it belongs. In

fact, it's worse than that. Sometimes the <LINK> is before the

<!DOCTYPE>. In addition, ampersands in URIs are *not* escaped as &#38;

The pages are sufficiently garbled to give even HTML Tidy a headache,

which makes it difficult to replace expect queries with wget queries.

(6) Nowhere in any of the pages is there the slightest mention of Javascript

or that you must turn off security features to use the pages. But

Javascript there is. You can imagine how thrilled I am at having to

enable Javascript on the machine where I write exams...

But here's the really cute thing. Under the old system, if I wanted to reserve a book, I had to enter my library card barcode and a password. As far as I know, the library card barcode wasn't used for anything else, and if someone intercepted the barcode and password, it didn't actually let anybody *do* anything to me except reserve books, which would have been nuisance value. Now all the staff have been assigned a user code and a password. The user code has the form <3 letters of last name> <2 letters of first name> <2 digits> <1 letter> I don't yet know how the final digits and letter are assigned. This user code is printed on the library cards, so at least all the library staff can see them. The password is not.

This is where social engineering comes in. Because these user codes and passwords are new, many staff members don't have them or don't know them. So you ring up a certain phone number, and they tell you what your password is or let you assign one. When I assigned my password last week, there was NO check that I was who I said I was.

Why is this a problem? After all, all you can do with this is reserve books and renew ones, plus see what someone has out, and I've always regarded what I have out as pretty much public information anyway.

The government here is introducing something called Performance Based Research Funding. Sounds good, except that the data are going

in now and won't be updated until 2006, so it's really (*Former* Performance) Based Research Funding. Most academic staff have to use a web browser to enter a lot of information (much of which the university should have anyway, but that's another story) into a PBRF database. How do they know you have a right to enter this information? Why, from your user code and password, of course. The same user code that is printed on your library card and the same password which is set/reported without any checks on who you are.

After that, I don't suppose I need to tell you that the courseware system uses the same user code and password as the other system.

[I somewhat reluctantly fixed a typo above: "bardcode" sounded appropriately Shakespearean for a library system. PGN]

✶ GenCon Registration Woes Blamed on Computer Network

<Allan Goodall <agoodall@att.net>>

Mon, 11 Aug 2003 09:06:53 -0500

GenCon is a large, annual game convention and trade show held at the end of July or early August. Although it was held in Milwaukee, Wisconsin for many years, this was its first year in Indianapolis, Indiana, with a record attendance figure of 28,000 people over the four days of the convention.

The wait in line to register has always been a point of complaint, but this

year that wait was particularly excessive, peaking at four hours on the Saturday. In an open letter to various message boards and newsgroups, GenCon CEO/owner Peter Adkison blamed most of the problem on the convention's computer network. A copy of the open letter can be found here: <http://www.gamingreport.com/article.php?sid=9515>

In summary:

- The computers used for registration were on the same network as the computers that allowed convention attendees to freely access the Internet. Apparently there were no restrictions on the use of these public access computers.
- By the first day of the convention 216 computers on the network were infected by a worm. The source of the infection was one of the public access computers, which also contained downloaded p*rn files.
- The network wasn't sufficient to handle the traffic even without the worm problem. The worm amplified the problem.
- Each attendee received a badge with their name printed on it. Badges were printed at a limited number of printers, 6 badges to a sheet. At times, the printers would time out due to the excessive network traffic. Sometimes the printed sheets would get lost. The badge printers were a major bottleneck in the system.

The RISKS here should be obvious.

This isn't the first time GenCon has had public access terminals on their network. The registration process doesn't appear to be much different from when I last attended (August 2000). Either the convention organizers were

unusually lucky in previous years, or the problems weren't deemed sufficiently bad to warrant (in the minds of the organizers) stronger security and procedural changes. Adkison doesn't state whether or not the change in venue this year was a contributing factor.

✶ Re: Metadata in Photoshop files ([RISKS-22.83](#))

<Sidney Markowitz <sidney@sidney.com>>

Fri, 08 Aug 2003 10:35:25 +1200

Photoshop may not be to blame and the RISK may be broader than a single software product being the Microsoft Word of photography.

According to Sue Chastain at

http://graphicssoft.about.com/b/a/2003_07_26.htm

the revealing thumbnails mentioned in [RISKS-22.83](#) were not likely to be

placed by Photoshop. Thumbnail previews, part of the EXIF metadata standard

used by all digital cameras, may be created automatically when the picture

is taken. She says "EXIF information and metadata is increasingly becoming a

concern for professional photographers working in digital because it can

potentially expose information [...]". Photoshop, rather than being the

culprit, has a "Save for Web" command that strips out metadata including

thumbnail previews.

⚡ Re: New online futures market bets on next White House scandal

<"Stephen R. Holmes" <srh@myrealbox.com>>

Fri, 8 Aug 2003 17:04:27 -0400

Having just re-read John Brunner's 1975 novel "The Shockwave Rider", I was, umm, shocked to open [RISKS 22.83](#) and find "New online futures market bets on next White House scandal" and "Pentagon's online trading market plan draws fire".

In Brunner's future world (circa 200x), citizens gamble on the "Delphi" odds that such-and-so (everything from war and famine to soap opera events) will come to pass, in exactly the same fashion. Both schemes mentioned in RISKS could have been taken directly from the novel.

Life imitating art?

⚡ Re: Software violates stock ownership limits ([RISKS-22.83](#))

<johnl@iecc.com (John R. Levine)>

8 Aug 2003 04:33:56 -0000

About 25 years ago, someone had a computer hooked up to a Telex line and programmed it to trade commodities futures, sending telex orders to his broker. But it wasn't programmed to take into account the size of the various markets, some of which aren't all that big, and one day he got a

phone call from the CFTC and they were not at all pleased that he had cornered the market in a thinly traded commodity, potatoes or something like that. He unwound his position and adjusted the program so it never traded that particular commodity again. I know this sounds like an urban legend, but I personally know the guy.

> For companies, the RISKS are less clear. It's not clear whether
> they had any way of finding out who was actually buying their stock, ...

Not really. Stock held in accounts at brokers or banks (most of it these days), is nominally owned by one of a handful of specialist companies such as Cede & Co. There is a way that the broker can tell the company who the beneficial owner is so they can send out annual reports and proxy statements, but that takes a while, so that companies have only a vague idea of who owns their stock on any given day. That's one of the reasons you have to file notices with the SEC if you plan to buy a substantial amount of a company's stock.

John R. Levine, IECC, POB 727, Trumansburg NY 14886 +1 607 330 5711
Member, Provisional board, Coalition Against Unsolicited Commercial E-mail



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

[ACM](#) Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 85

Friday 15 August 2003

Contents

- [Niagara-Mohawk power grid overload causes major outages](#)
- [Pilot fixes faulty jet](#)
[Chuck Weinstock](#)
- [ATM scam netted \\$620,000 Australian](#)
[John Colville](#)
- [Credit-card theft spam](#)
[Drew Dean](#)
- [New worm targets Microsoft security site](#)
[NewsScan](#)
- [Blaster worm analysis](#)
[Monty Solomon](#)
- [CERT Advisory CA-2003-20 W32/Blaster worm](#)
[Monty Solomon](#)
- [DCOM worm analysis report: W32.Blaster.Worm](#)
[Dave Ahmad](#)
- [FBI enters investigation of Blaster](#)
[NewsScan](#)
- [Re: Software patching gets automated](#)
[Fuzzy Gorilla](#)
- [Hidden risks: location dependence](#)

[Fuzzy Gorilla](#)

- [Another variant on deceptive URLs](#)
[Geoffrey Brent](#)
 - [Risks of globally filtering mail to IT and security staff](#)
[Aryeh Goretsky](#)
 - [Denver school information system on the Internet](#)
[Dave Brunberg](#)
 - [Biloxi schools have cameras in classrooms, pictures on Internet](#)
[Carl G. Alphonse](#)
 - [Beyond Fear, Bruce Schneier](#)
[PGN](#)
 - [CFP: RFID Privacy and Security Workshop @ MIT](#)
[Simson L. Garfinkel](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ **Niagara-Mohawk power grid overload causes major outages**

<"Peter G. Neumann" <neumann@csl.sri.com>>

Fri, 22 Aug 2003 07:01:11 PDT

A grid overload just after 4pm EDT knocked out power in NY City, Boston, Cleveland, Detroit, Toronto, and Ottawa, among many other cities, and spanning New York, New Jersey, Vermont, Connecticut, Pennsylvania, Ohio, Michigan, Ontario, and parts of Quebec. Much of midtown NYC and Wall Street were shut down. At least 10 major airports, causing schedule problems across the country and abroad. Nine nuclear power plants were shut down. Landline phones and cell circuits were severely affected, with extensive traffic saturation even where battery backups were available. At least 50 million people were affected. 800 trapped-in-elevator rescues.

For a while, a lightning strike on the US side of Niagara Falls was reportedly the trigger, and then attributed to a fire, although this morning the exact cause is still mysterious -- with one power expert suggesting "somewhere in the midwest". Terrorism is ruled out, but not apparently not yet cyberactivity. All this supposedly happened in nine seconds, and yet the cause is still unclear! (My summary is of course **not** a definitive report.)

Once again this should certainly be instructive from a RISKS point of view.

Despite the experience gained from past power-outage propagations, plus the unrelated but propagationally similar 1980 complete ARPAnet collapse and 1990 nationwide AT&T collapse, we still have a lot to learn. Each time we get a widespread effect of this nature, the people who keep saying that this kind of propagation is impossible get serious egg on their faces. Stay tuned for more detailed analyses and more discussion of what it takes to have seriously defensive/preventive design and implementation.

One quote from New Mexico governor Bill Richardson is intriguing: "We're a superpower with a Third World grid."

✈ Pilot fixes faulty jet

<Chuck Weinstock <weinstock@sei.cmu.edu>>

Tue, 12 Aug 2003 10:34:20 -0400

A pilot personally fixed a faulty plane stranded on Spain's Balearic island of Menorca before getting weary British tourists to vote on whether they wished to be flown home aboard the repaired jet. The incident occurred on 8 Aug 2003 after a Boeing 757 run by British tour operator MyTravel was found to have a faulty onboard computer that insisted the aircraft was airborne when it was in fact parked on the tarmac. Covered in oil after resetting a sensor in the aircraft's nosewheel, the pilot asked passengers gathered in the airport's terminal to raise their hands if they wished to board the plane. In the end, only 13 of nearly 200 tourists decided to stay put.
[Source: AFP, 12 Aug 2003, from *The Times* (London); PGN-ed]

✶ ATM scam netted \$620,000 Australian

<colville@it.uts.edu.au>

Tue, 12 Aug 2003 08:56:06 +1000

ATM swipe-and-snap scam netted A\$620,000, court told
Leonie Lamont, 12 Aug 2003, *Sydney Morning Herald*, 12 Aug 2003; PGN-ed

<http://www.smh.com.au/articles/2003/08/11/1060588322961.html>

[\$A620,000 is about \$US400,000.]

In the first case of its kind in Australia, a man has pleaded guilty to defrauding more than A\$623,000 from bank customers by electronically spying on them while they used ATMs. Kok Meng Ng, 29, a Malaysian, admitted in the District Court yesterday to taking part in an elaborate scheme

in which an electronic skimming device and pin-head camera were planted in 36 ATMs in Sydney. The skimming devices read the data on the magnetic stripe on customer's cards, while the camera recorded the PINs as they were punched in, beaming a signal that could be received up to 400 metres away.

On 64 occasions between May 2001 and November last year, Ng, who was in Australia on successive tourist visas, transferred amounts of less than A\$10,000 to overseas accounts. Amounts over A\$10,000 must be reported by financial institutions. The court heard that among the incidents, the scam was conducted on 15 Oct 2002 on a St George ATM in Darlinghurst, a Westpac machine in Bondi Junction a day later, and, four days later, on a Commonwealth Bank ATM in Chatswood.

The prosecutor, Sunil de Silva, said Ng was part of a gang that raided the bank accounts of 315 people, generally withdrawing less than A \$1000. Ng also pleaded guilty to federal charges under the Financial Transactions Act. The federal charges carry a maximum five year jail term, and the computer crime charges a three year term. ...

John Colville, Dept of Computer Systems, University of Technology, Sydney AU
PO Box 123, Broadway NSW Australia 2007 +61-2-9514-1854
colville@it.uts.edu.au

✶ Credit-card theft spam

<Drew Dean <ddean@csl.sri.com>>

Thu, 14 Aug 2003 12:38:08 -0700 (PDT)

I've recently received a couple pieces of spam trying to induce me to give out my credit-card number. One used a lot of artwork from PayPal, and even referenced PayPal's privacy policy. The biggest problem with it (besides the decidedly non-PayPal domain the form was submitted to, of course :-)) is that I don't have a PayPal account.

Interestingly, neither spam used https to actually submit the form. This makes one wonder about the RISK: what a machine to crack and to steal credit-card numbers from! The operators of the scam can hardly go to law enforcement, after all. The owners of the machine, if it's a Web-hosting service, might be able to go to law enforcement, although it would rather embarrassing for them.

Drew Dean, SRI International, Computer Science Laboratory

🚀 New worm targets Microsoft security site

<"NewsScan" <newsscan@newsscan.com>>

Tue, 12 Aug 2003 11:19:20 -0700

A virus-like computer attack expected to infect hundreds of thousands of computers worldwide is programmed to direct all infected computers to attack the security-related Microsoft Web site www.windowsupdate.com,

used by millions of Microsoft users each week. The worm, variously called LoveSan, Blaster and MSBlaster, is apparently similar in structure to the Code Red virus that affected 300,000 computers two years ago; it targets a flaw in Microsoft Windows operating systems, and is considered to be a worm type of virus because it doesn't require computer users to open an e-mail attachment or take any other action to spread automatically from computer to computer. Home computer users who leave computers constantly online to the Internet through DSL or cable are among those most at risk. [*San Jose Mercury News 11 Aug 2003; NewsScan Daily, 12 Aug 2003]
<http://www.siliconvalley.com/mld/siliconvalley/6511962.htm>

Blaster worm analysis

<"monty solomon" <monty@roscom.com>>
Tue, 12 Aug 2003 15:02:01 -0400

Blaster Worm Analysis
Release Date: 11 Aug 2003
Severity: High

Description: The Blaster worm uses a series of components to successfully infect a host. The first component is a publicly available RPC DCOM exploit that binds a system level shell to port 4444. This exploit is used to initiate a command channel between the infecting agent and the vulnerable target. Once the target is successfully compromised, the worm

transmits the
msblast.exe executable (the main body of the worm) via TFTP to
infect the
host. The payload used in the public DCOM exploit, as well as
the TFTP
functionality, are both encapsulated within msblast.exe.

<http://www.eeye.com/html/Research/Advisories/AL20030811.html>

✶ CERT Advisory CA-2003-20 W32/Blaster worm

<"monty solomon" <monty@roscom.com>>

Tue, 12 Aug 2003 15:05:56 -0400

CERT Advisory CA-2003-20 W32/Blaster worm

Original issue date: August 11, 2003

Last revised: August 12, 2003

Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- * Microsoft Windows NT 4.0
- * Microsoft Windows 2000
- * Microsoft Windows XP
- * Microsoft Windows Server 2003

Overview

The CERT/CC is receiving reports of widespread activity related to a new piece of malicious code known as W32/Blaster. This worm appears to exploit known vulnerabilities in the Microsoft Remote Procedure Call (RPC) Interface.

I. Description

The W32/Blaster worm exploits a vulnerability in Microsoft's DCOM RPC interface as described in VU#568148 and CA-2003-16. Upon successful execution, the worm attempts to retrieve a copy of the file msblast.exe from the compromising host. Once this file is retrieved, the compromised system then runs it and begins scanning for other vulnerable systems to compromise in the same manner. In the course of propagation, a TCP session to port 135 is used to execute the attack. However, access to TCP ports 139 and 445 may also provide attack vectors and should be considered when applying mitigation strategies. Microsoft has published information about this vulnerability in Microsoft Security Bulletin MS03-026.

Lab testing has confirmed that the worm includes the ability to launch a TCP SYN flood denial-of-service attack against windowsupdate.com. We are investigating the conditions under which this attack might manifest itself. Unusual or unexpected traffic to windowsupdate.com may indicate an infection on your network, so you may wish to monitor network traffic.

Sites that do not use windowsupdate.com to manage patches may wish to block outbound traffic to windowsupdate.com. In practice, this may be difficult to achieve, since windowsupdate.com may not resolve to the same address every time. Correctly blocking traffic to windowsupdate.com will require detailed understanding of your network routing architecture, system management needs, and name resolution environment. You should

not block
traffic to windowsupdate.com without a thorough understanding of
your
operational needs.

We have been in contact with Microsoft regarding this
possibility of this
denial-of-service attack. ...

<http://www.cert.org/advisories/CA-2003-20.html>

⚡ DCOM worm analysis report: W32.Blaster.Worm

<Dave Ahmad>

Mon, 11 Aug 2003 15:36:24 -0600 (MDT)

A Bugtraq user has already pointed out that a worm has been
discovered in the wild that exploits the Microsoft Windows DCOM
RPC

Interface Buffer Overrun Vulnerability (Bugtraq ID 8205) to
infect

host systems. Symantec has been tracking its activity and is
currently conducting analysis/full disassembly of the malicious
code,
which has been named "Blaster". The results of our analysis are
being made available to the public at the following location:

<https://tms.symantec.com/members/AnalystReports/030811-Alert-DCOMworm.pdf>

It is expected that this report will be updated frequently as
more
information is discovered. Readers are advised to download/
refresh
it throughout the day to ensure that any new information is not
missed.

David Mirza Ahmad, Symantec

🔥 FBI enters investigation of Blaster

<"NewsScan" <newsscan@newsscan.com>>

Thu, 14 Aug 2003 08:46:52 -0700

The FBI is investigating the origin of the malicious computer program Blaster (also known as MSBlaster and LoveSan), which has already wormed its way into more than 250,000 Internet-connected computers running Windows software. Blaster has been infecting computers in organizations of every kind (e.g, CBS, the Senate, and the Federal Reserve Bank of Atlanta) -- in spite of the fact that computer experts say it's not well-written software.

Dan Ingevaldson of Internet Security Systems Inc. warns: "A better version of this worm wouldn't crash any machines; it would work correctly every time, move faster, and delete or steal its victims' files." [*The

Washington Post*, 14 Aug 2003; NewsScan Daily, 14 Aug 2003]

<http://www.washingtonpost.com/wp-dyn/articles/A56071-2003Aug13.html>

🔥 Re: Software patching gets automated ([RISKS-22.84](#))

<"Fuzzy Gorilla" <fuzzygorilla@euroseek.com>>

Tue, 12 Aug 2003 12:23:22 -0400

In <http://catless.ncl.ac.uk/Risks/22.84.html#subj11.1> Peter Neumann

speculates: "And when it is *fully* automated, think of how wonderful

it will be to have new Trojan horses and security flaws installed instantaneously, without having to require human intervention."

Even without Trojan horses and security flaws, it introduces yet another point of failure into the system, as evidenced by the "Blaster" worm.

According to a New Scientist article "Computer worm attacks software patch

server" <http://www.newscientist.com/news/news.jsp?id=ns99994046> :

After infecting a vulnerable computer, the worm is programmed to send a

volley of bogus traffic to Microsoft's software update service, windowsupdate.com on 16 August. If enough machines are infected this will

overwhelm the site, preventing system administrators from using it to

download the software patches needed prevent other machines being

infected. "It's an extremely devious trick by Blaster's author," says

Graham Cluley, of UK anti-virus company Sophos. "Blaster attempts to knock

Microsoft's windowsupdate.com Web site off the Internet."

Hidden risks: location dependence

<"Fuzzy Gorilla" <fuzzygorilla@euroseek.com>>

Tue, 12 Aug 2003 13:03:31 -0400

Although this example comes from biology rather than computers, I think it

helps to point out the problem of hidden risks and the value of

questioning assumptions. Basically, a researcher was working on a study that showed a strong link between cholesterol and an Alzheimer's like disease in rabbits -- until he changed the location of his lab.

Sparks has been working with rabbit models of Alzheimer's for years.

"Every time I ever fed a bunny cholesterol, I got Alzheimer's pathology," he said.

That is, until he moved to the Sun City lab.

"I said, 'Something is wrong. I go down into the vivarium (where lab animals are kept) and the first thing I see is the wall being lined with big blue bottles.'"

It turns out the rabbits there were given distilled water, while all the other research animals Sparks had worked with got tap water.

He analyzed the tap water from previous labs and found it contained copper. When the rabbits at Sun Health were fed tap water, they also developed Alzheimer's symptoms.

When Sparks added copper to the distilled water and gave the rabbits cholesterol, they also developed Alzheimer's-like symptoms and brain lesions.

<http://asia.reuters.com/newsArticle.jhtml?type=healthNews&storyID=3258703>

Just as in biological systems, computers and computer networks are very complex and sometimes the variables are well hidden.

✂ Another variant on deceptive URLs

<Geoffrey Brent <g.brent@student.unsw.edu.au>>

Thu, 14 Aug 2003 09:51:46 +1000

Another refinement of the "please click this link and log into your financial Web site" scam. This morning I got one purporting to be from Westpac Australia. Obviously a fraud, since (a) legitimate institutions don't do business that way, and (b) I don't have an account with them. But it still took me a moment to see how this one worked.

The link given in the e-mail purported to be "<https://olb.westpac.com.au>" (Westpac's online banking site). I was curious to see how this one worked, so I did what I usually do with such hoaxes and ran the mouse over it. I expected to see a completely different URL show up in the status bar, or perhaps something along the lines of "...westpac.com.au@scammer.url.etc" and was rather surprised to see what looked to be a genuine Westpac URL, differing only in being HTTP rather than HTTPS: <http://olb.westpac.com.au/> -- which, although unencrypted, would still be owned by Westpac.

In fact, on looking closer, the `_real_` URL is:

```
http://olb.westpac.com.au%20%20%20%20[lots more space
characters snipped]
:UserSession%3D2f4d0zzz899amaiioiibv5589955&userrstste
%3DSecurityUpdate&StateLevel%3DCameFrom@european.website29.
```

ebizdns.com/

The spaces ensure that the interesting bits in the link don't show up onscreen, and since one doesn't expect to see spaces in URLs it wasn't something I'd expected. (And yes, I missed the ... on the RHS of the bar that indicated that there was more to follow). AFAICT, the http/s mismatch is simply sloppiness on the culprit's part rather than a necessary part of the scam.

I can't be the first to point this out, but: having a character that is visually indistinguishable from the absence of a character is in itself a risk. Perhaps it would be useful for URL-display and similar outputs to use a visible character to indicate spaces, as can be done with word-processors?

✶ Risks of globally filtering mail to IT and security staff

<Aryeh Goretsky <goretsky@adelphia.net>>

Wed, 13 Aug 2003 02:43:40 -0600

Earlier this evening I received a message in my in-box advertising an organic compound which, allegedly, would increase the dimensions of a particular body part.

Such unsolicited messages are quite commonplace these days and a quick perusal of the message header revealed nothing especially interesting about the message.

What did surprise me, though, was the sender's choice of a falsified return address from the americanexpress.com domain. Knowing financial institutions are very sensitive to misuse of their names I forwarded a copy to "abuse@americanexpress.com" with a self-explanatory subject and a concise, one-line description of what the message was and I why I had forwarded it.

I received the following automated reply (unimportant headers removed):

```
> Date: Sat, 09 Aug 2003 03:17:53 -0700
> From: no.reply@aexp.com
> To: "Aryeh Goretsky" <goretsky@adelphia.net>
>
> Subject: Inappropriate Language Notification
>
> A communication sent from your e-mail account was
> intercepted and quarantined because it contained language
> deemed inappropriate for business communications. If
> you feel your message was quarantined in error,
> please contact the intended recipient.
>
> Sender: Aryeh Goretsky <goretsky@adelphia.net>
> Subject: spam sent with forged address
> Date: 08/09/2003, 03:17:53 AM
> Policy: Inappropriate Language
```

As someone who provided technical support in the security field for a long time I regularly received messages with "inappropriate" language in them, usually in the form of messages contained in computer viruses, worms and the like. As a security professional, I **needed** to know the exact message as it appeared on-screen or embedded in a program in order to help isolate and

identify the problem.

Frankly, the idea of *not* being able to gather this information because that someone, somewhere might see "inappropriate" language floored me.

I understand that large companies such as American Express cannot afford to vet new IT hires, let alone existing ones, for a good organizational fit which among other things includes not being offended by "inappropriate" language, but the idea that someone whose job responsibilities may require viewing such information and not being able to see it strikes me as willful misconduct by whatever employee(s) came up with such a policy in the first place.

Perhaps organizations which perform such filtering should provide staff whose job requirements required them to receive messages containing "inappropriate" language with a waiver.

In the meantime, I can't help but wonder what would happen if someone defaced one of American Express's web servers with a message containing "inappropriate" language and none of their IT or security staff were able to coordinate a response due to their internal communiques being rejected.

The *RISKS* seem obvious.

[... but not surprising. I have had so many such requests to sites bounced for similar reasons. PGN]

[True, but I assume (with all problems thereof) a higher

level of

accountability from the security/fraud unit of a financial institution.

AG]

✶ Denver school information system on the Internet

<Dave Brunberg <DBrunberg@FBLEOPOLD.com>>

Thu, 14 Aug 2003 09:33:03 -0400

I found this link to an article about Denver's "Internet Student Information System," which offers parents (or anyone with a userid/password combo) to view their children's (targets'?) whereabouts, grades, disciplinary records, and demographic info online.

<http://www.denverpost.com/Stories/0,1413,36~53~1569401,00.html>

Teachers enter class attendance data into the system at the beginning of each class, and "Almost on an hourly basis, a parent can find out if their child is in a particular class. Most schools will stick to updating attendance two or three times a day." "While the systems differ, they share a concern for security with school-issued user IDs and passwords. " "If [parents] want to participate, they must take a photo ID to the school and then they are given a user ID and personal password. They have access only to their children's information."

Sounds really secure, no? No word on the form of userid or password, or how

to change the password, etc., standard RISKS apply. Near the end of the article, security and privacy issues are given a brief note:

"Like Castagna at Lakewood High, Bailey said no concerns have been raised

about privacy, and nobody's information has been hacked.

David Craven,

Cherry Creek's director of instructional technology, said the systems use

the same safeguards as online banking. "People have an expectation to get

general information on the Web. It's just part of their lives."

"The value is contingent on how secure the database is," said Stephen

Keating, director of the Privacy Foundation at the University of

Denver. "If the school district thinks they've got it protected so that

only the parents or the student can get access to that student's

information, then it sounds viable." But, he cautioned, "just because you

think it's secure doesn't mean it is."

Mark Silverstein, legal director of the American Civil Liberties Union in

Denver, said, "If the information is only available to the parents of a

student, I don't see what the concern is about privacy."

I'll take a brief quote from that to look at again: "If the school district

thinks they've got it protected so that only the parents or the student can

get access to that student's information, then it sounds viable." Um,

shouldn't the district KNOW they've got it protected? Shouldn't they be

actively trying to crack the system? Maybe they can ask some of their

brighter 10th graders to try--that would probably open up some interesting discussion when the results became known. Anyone want to take a bet on how many Mountain Dews it takes to crack this one?

David W. Brunberg, Engineering Supervisor, The F.B. Leopold Company, Inc.,
227 South Division Street, Zelienople PA 16063 (724) 452-6300

⚡ Biloxi schools have cameras in classrooms, pictures on Internet

<"Carl G. Alphonc" <alphonc@cse.Buffalo.EDU>>

Wed, 13 Aug 2003 20:28:37 -0400

According to a CNN article

<http://www.cnn.com/2003/EDUCATION/08/12/classroom.cameras.ap/index.html>

the Biloxi, Mississippi school district has put cameras in all of its classrooms. The project was funded by casino revenues. Pictures taken by the cameras are viewable on the Internet. If the article is correct, and the images really are accessible from anywhere on the Net, the risks of others viewing the pictures is real.

The article does not give much motivation for installing the cameras. It states, "[Deputy superintendent] Voles said the camera installation is a precaution, and that students and teachers have said they feel safer." The potential for abuse and the potential chilling effect on the classroom is left as an exercise for the reader. I wonder, might the introduction of

these cameras perhaps backfire, attracting those who seek publicity, since they are guaranteed a record of their activities?

Carl Alphonse, Dept of Computer Science and Engineering
University at Buffalo, Buffalo, NY 14260-2000

Beyond Fear, Bruce Schneier

<"Peter G. Neumann" <neumann@csl.sri.com>>

Fri, 15 Aug 2003 07:01:44 PDT

Beyond Fear: Thinking Sensibly about Security in an Uncertain World

Bruce Schneier

Copernicus Books (a Springer-Verlag imprint)

ISBN 0-387-02620-7

<http://www.schneier.com/bf.html>

Copernicus was a Polish astronomer who observed that the Earth rotates on its axis and revolves around the Sun. That knowledge was absolutely heretical at the time.

Bruce Schneier is a security guru who generally preaches common sense (a common theme in RISKS, although common sense is apparently surprisingly uncommon overall). In our time, common sense may seem absolutely heretical to people other than those of us who try to practice it. Fortunately, RISKS readers seem to be much more aware than nonreaders. For those of you who think you believe in common sense, this book will strongly reinforce your beliefs -- and will do so quite entertainingly. On the other

hand, those
who do not actually practice what we preach here had better read
Bruce's
book very carefully.

✶ CFP: RFID Privacy and Security Workshop @ MIT

<"Simson L. Garfinkel" <slg@ex.com>>

Wed, 13 Aug 2003 20:05:19 -0400

RFID PRIVACY AND SECURITY -- WORKSHOP @ MIT -- CALL FOR
PARTICIPATION

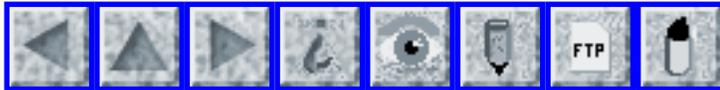
Saturday, 15 Nov 2003, 10am - 4pm, Bartos Theater, MIT Media
Lab, 20 Ames St.

Radio Frequency Identification technology is fast becoming a
lightning rod
for consumer privacy activists. Is RFID destined to become the
enabling
technology for massive state-sponsored surveillance, Big
Brother's
"call-home" chip? Or is RFID really nothing more than a supply-
chain
management technology, its dangers being over-hyped by alarmists
who
fundamentally misunderstand the technology? One thing is sure:
in the
absence of strong data, decisions are being made and the public
is either
being poorly informed or intentionally misled.

Last year Benetton pulled back from a previously-announced RFID
trial after
a consumer group announced a global boycott of the clothing
manufacturer.
Can pressure from consumer groups effectively prevent the
introduction of
RFID technology, or were other matters at work behind the scenes?

The goal of the RFID Privacy Workshop is to bring together RFID technologists, boosters, critics, privacy activists and journalists covering the space to establish some technical truths and a creating a framework for understanding the growing body of RFID policy issues.

To register online and/or submit a paper by 15 Sep 2003, see <http://www.rfidprivacy.org/>



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

[ACM](#) Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 86

Sunday 17 August 2003

Contents

- [Of course, it couldn't happen again!](#)
[PGN](#)
- [The Road to Vulnerability](#)
[Patrick Lincoln](#)
- ["Blackouts and Bush's Buddies"](#)
[Lauren Weinstein](#)
- [Internet stays light during blackout](#)
[NewsScan](#)
- [Re: Power-grid overload](#)
[Declan A Rieb](#)
[Edward Reid](#)
[Jonathan Kamens](#)
- [msblast and the power failure?](#)
[William Ehrich](#)
- [Flaw seen in patch by Microsoft](#)
[Monty Solomon](#)
- [Blaster Worm vulnerability](#)
[Michael Smith](#)
- [Bug downs Australian pay phones](#)
[Fuzzy Gorilla](#)

- [Free Software Foundation hacked](#)
[Patrick Lincoln](#)
 - [Nasdaq reports incorrect pricing](#)
[Fuzzy Gorilla](#)
 - [Legit website or nefarious scam?](#)
[Matt Anderson](#)
 - [easynet.nl is causing serious e-mail disruption](#)
[Jim Garrison](#)
 - [Re: Another variant on deceptive URLs](#)
[John Stockton](#)
 - [Re: Identity Crisis and *The Washington Post*](#)
[Rob Slade](#)
 - [bardcode](#)
[Jamie Zawinski](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✂ Of course, it couldn't happen again!

<"Peter G. Neumann" <neumann@csl.sri.com>>

Sun, 17 Aug 2003 09:14:13 PDT

There are still a lot of unknowns, several days later. A current theory on the 14 Aug 2003 Northeast blackout attributes what started the cascade effect to human failure to respond properly to an alarm denoting the failure of transmission lines (including a tree in contact with a power line) near Cleveland at 3:06pm -- over an hour before the massive nine-second propagation. According to the front page of **The New York Times**, 17 Aug 2003, "It is not clear whether the problem with the alarm delayed action by the utility, FirstEnergy Corporation, or the consortium that controls the

regional grid, the Midwest Independent System Operator."

The same article notes that the newly released timeline of the North American Electric Reliability Council (investigating the blackout) does not answer how a local failure "could have spread catastrophically to other regions, overwhelming mechanisms designed to halt such a spread."

Note the similarity with the massive *West* Coast grid blackout on 2 Jul 1996 in which a tree touched a power line, and the operator who had detected an anomaly could not find the phone number required for the manual alert. And then of course, there were numerous claims that such a massive outage could not happen again -- until the 8-state collapse on 10 Aug 1996! (See [RISKS-18.27](#) to [29](#) and especially [RISKS-22.32](#), on "why it couldn't happen again"!) Rather than harp on the lessons that need to be learned, let me suggest that you read Pat Lincoln's thoughtful piece, which follows.

⚡ The Road to Vulnerability (Re: Blackout, [RISKS-22.85](#))

<Patrick Lincoln <lincoln@csl.sri.com>>

Fri, 15 Aug 2003 17:09:33 -0700

One lesson that can be drawn from incidents like the recent massive power outage is that decreasing margins in all our infrastructures place critical societal functions at greater and greater risk of significant disruptions

from rare accidental and malicious acts. Redefining acceptable levels of risks and protections as the world changes is hard work, but need to be done.

Cost pressures and tight engineering under benign assumptions lead to thin margins. Optimized engineering leads to most events being of small consequence (we've engineered systems to tolerate them), but some rare events can cause massive disruption. It would be 'bad engineering' to overdesign a system to tolerate very rare events, if that tolerance costs more than the failures it would prevent (in expected value to customer terms). Fragility to extremely rare events can be seen as good business. It would be surprising if there weren't rare disruptions (like massive power outages) in highly optimized infrastructures.

But the invisible hand of economics and good engineering leave systems designed and optimized under assumptions of relatively benign environments at great risk if new or unexpected threats arise.

Computer systems change very rapidly, and new threats arise with disturbing speed. The current hardware manufacture, software development, and people practices of our cyber infrastructure are obviously subject to the same economic motivations as described above. So they are already (and will become even more) fragile to rare or unexpected accidental or malicious events. That's 'good business' paving the road to vulnerabilities.

Post 9/11, we can point out how previously almost unthinkable scenarios are more thinkable now, and thus engineered defenses against potential attacks are more strongly motivated. Govt procurement practices, corporate and individual liability, government mandates, and other mechanisms could have a profound impact on the reliability and cost of cyber infrastructure, but also on large-scale economic concerns, so it may be imprudent to act without defining the threats. To define and quantify cyber threats and their impact, particularly in combination with coordinated physical and psychological attacks and effects, requires deep (read: expensive) contemplative research, development, large experimentation, etc. Once new threats and defenses are defined, all the costs associated with deployment of those mechanisms can be at least partially quantified, and then well-reasoned decisions can be made about appropriate levels of protection against various risks. The pace of technology change and societal reliance on these systems amplify the uncertainty, urgency, and magnitude of risk here. It is almost unthinkable that western societies would not put very large resources against a problem of this grave potential.

✶ "Blackouts and Bush's Buddies" (Re: Blackout, [RISKS-22.85](#))

<Lauren Weinstein <lauren@vortex.com>>

Thu, 14 Aug 2003 22:26:09 -0700

Many of the reports on today's blackout have expressed the view that it comes as a complete surprise.

The reality of course is that such a blackout was entirely expected by those who follow the power industry, as I discuss in the new short audio (mp3) Fact Squad Radio feature, "Blackouts and Bush's Buddies."

It's playable via:

<http://www.factsquad.org/radio>

Lauren Weinstein, lauren@pfir.org <http://www.pfir.org/lauren>
Moderator, PRIVACY Forum - <http://www.vortex.com> Tel: +1 (818)
225-2800

[Also, see System's Crash Was Predicted:

<http://www.washingtonpost.com/wp-dyn/articles/A61117-2003Aug15.html>

PGN]

Internet stays light during blackout

<"NewsScan" <newsscan@newsscan.com>>

Fri, 15 Aug 2003 09:53:41 -0700

During yesterday's blackout in northeast U.S. states and several major Canadian cities, wireless networks and Internet connections allowed people to keep communicating. The chief business officer of Equinix, which operates Internet Business Exchange centers that serve more than 90% of the world's Internet routes, explains: "We lost all utility power out there, but we immediately went to battery power for a few seconds, at which

point all
of our major generators kicked in" to allow normal operations
that were
"totally seamless to customers." Internet customers therefore
suffered "no
disruptions whatsoever" to their Internet service resulting from
the
electrical system failures. [AP/*San Jose Mercury News*, 15 Aug
2003;
NewsScan Daily, 15 August 2003]
<http://www.siliconvalley.com/mld/siliconvalley/6540489.htm>

⚡ Re: Power-grid overload ([RISKS-22.85](#))

<"Declan A Rieb" <darieb@sandia.gov>>
Fri, 15 Aug 2003 15:59:26 -0600

Quoting [with permission] a colleague in a hallway conversation:

Review of yesterday's lesson:

Q. What is the ONE critical Infrastructure? [upon which all the
others depend]

A. Electricity

Q. What is its most salient feature?

A. Nobody knows how it works. [Or perhaps more correctly, how it
DOESN'T work.]

Declan A Rieb, <darieb@sandia.gov>, 505 845-8515
Sandia National Laboratories MS1202, Albuquerque NM 87185-1202

⚡ Re: Power-grid overload ([RISKS-22.85](#))

<Edward Reid <edward@paleo.org>>

Sun, 17 Aug 2003 00:04:24 -0400

> All this supposedly happened in nine seconds, and yet the
cause is still
> unclear!

The very fact that it happened so fast is one reason that expert speculation on the cause has been slow to come. (Political speculation, of course, occurred almost as fast as the outage.) Most large outages, including the ones in the northeast US in 1965 and 1977, propagated over a period of many minutes. They involved overloads which did not immediately trip protection. The symptoms were such that the (human) system operators were expected to see them and react, and the failure of the operators to shed load quickly was a major factor in the extent of the outages.

By contrast, this outage spread so fast that only automatic controls had any chance of stopping it once it began. (Whether recognizably dangerous conditions existed before the first failure remains to be seen. Analysis of contingencies is a major part of online control systems, but choosing the proper actions to minimize risk is an extremely complex problem.) In those outages decades ago, the system was gradually pulled over the brink. In this outage, it was tossed over the edge like a finger flicking a match stick. The Niagara area saw a flow change of 3GW, the output of three nukes, in under a second.

We're already hearing "we will put changes in place so that this will not happen again". But a system operator who has spent eight hours a

day for the past 25 years keeping a system up -- successfully -- needs more than a few seconds to shift mindset and do the almost unthinkable -- shed load -- to protect the system, even when the signs are clear. Problems of this nature are so rare that we do not, cannot, trust either the humans or the computers. Perhaps the best action would be to provide effective simulators so that the operators can spend a few hours a week reminding themselves of what a real emergency feels like. But most likely we will see proposals which leave the humans out of the loop.

Of course, certain technical measures would help. So far, the newspaper analyses of the outages correctly point out limited transmission capacity as a problem. Deeper problems are the anti-regulatory environment, that safety doesn't sell, and the failure to invest in conservation.

Building "excess" transmission capacity has no market incentive. Excess capacity is essential to safety, but safety doesn't sell. The market calls it excess capacity; people call it a safety net. When a critical line fails, parallel lines must have "excess" capacity to take over the flow, and this safety net must remain intact when lines are out of service for maintenance. Safety nets are not cheap.

Conservation is far more cost-effective than new construction at ensuring continuous availability of electricity. But this is not a market-savvy investment, so until we accept that we need non-market investments in conservation, we will continue to waste our most effective

resource.

⚡ Re: Power-grid overload ([RISKS-22.85](#))

<Jonathan Kamens <jik@kamens.brookline.ma.us>>

Fri, 15 Aug 2003 11:10:50 -0400

> A grid overload just after 4pm EDT knocked out power in NY
City, Boston,
> Cleveland, Detroit, Toronto, and Ottawa, among many other
cities,

For the record, Boston did not lose power. According to the
*Boston
Herald*, the only cities in Massachusetts that lost power were
Pittsfield
and Springfield. I don't know first-hand whether that
information is
accurate, but I do know that the greater Boston area, or at
least the
portions of it in which I and my coworkers traveled yesterday,
never lost
power.

⚡ msblast and the power failure?

<William Ehrich <ehrich@mninter.net>>

Fri, 15 Aug 2003 17:42:51 -0500

Possible connection? Wild guess? I'm not competent to evaluate
this:

<http://www.heise.de/newsticker/data/ju-15.08.03-001/> [in
German]

[The cited article is written by Juergen Schmidt, senior editor of heise, which publishes c't, which we have quoted in RISKS before. (See <http://www.heise.de/ct/impress.shtml> ; tel +49 511 53 52 300.)

Basically, this article notes that National Grid is a "reference client" of Northern Dynamics, and that OPC uses COM/DCOM, and that this is precisely the technology that the Blaster worm trashes. It does not *claim* that OPC was used for any of the SCADA applications that might have triggered the propagation, but merely raises the question of whether this might have been the case. The possibility is not too far fetched, especially if the common flaw existed in multiple distributed computerized control systems. ADDED NOTE, *The International Herald Tribune* has a story this weekend on MS shutting down www.windowsupdate.com saying that "Security experts say they have found no evidence that the blackout ... was related" to Blaster. But then so much else is unclear, so who knows? Thanks to Peter Ladkin for providing background on this. PGN]

✶ Flaw seen in patch by Microsoft

<"monty solomon" <monty@roscom.com>>

Fri, 15 Aug 2003 16:00:00 -0400

A program Microsoft instructed customers to use to fix a hole in its Windows software, which is vulnerable to attack by the Blaster/Lovsan

worm that infected computers this week, may itself be flawed. A glitch in the Microsoft Windows Update patch-management system used to download Windows software fixes has tricked some customers into thinking their systems were patched to prevent Lovsan, when they really were not, said Russ Cooper, moderator of a mailing list with 30,000 subscribers that tracks Microsoft's software weaknesses. ... [Source: CBS MarketWatch, 15 Aug 2003] <http://www.chron.com/cs/CDA/ssistory.mpl/business/2049216>

Blaster Worm vulnerability

<"Michael Smith" <emmenjay@zip.com.au>>
Sun, 17 Aug 2003 21:44:01 +1000

I recently received an e-mail from Microsoft, with the title: "Actions for the Blaster Worm - Special Edition, Microsoft Australia News and Events".

It contained (mostly useful) advice on dealing with the Blaster worm, but included this:

> Your computer is not vulnerable to the Blaster worm if
> either of these conditions apply to you:
>
> * If you are using Microsoft Windows 95; Windows 98;
> Windows 98 Second Edition (SE); or Windows Millennium (Me).
> * If you downloaded and installed security update MS03-026
> prior to 11 August 2003, the date the worm was discovered.

The second of these would be valid if we know for sure that the

worm was not
in the wild before it was discovered, but I don't see how we can
be
confident of that.

I would expect the rate of spread to be approximately
exponential, until the
net begins to become saturated. The worm might have been around
for days or
even weeks before it was formally "discovered".

Michael Smith, Aurema Pty Limited, PO Box 305, Strawberry Hills
2012, Australia
79 Myrtle Street, Chippendale 2008, Australia +61 2 9698 2322
www.aurema.com

🔥 Bug downs Australian pay phones

<"Fuzzy Gorilla" <fuzzygorilla@euroseek.com>>

Fri, 15 Aug 2003 12:59:07 -0400

[Ah, for the good old days of analog phones with dials.]
[Unfortunately, neither news report gives much in details
about the real
cause of the problem or why only some payphones are having
problems.]

In Australia, about half of Telecom's 5000 public payphones were
out of
order due to a software bug, and the situation is slow to
improve. Manual
reset of each phone may be necessary.

[Sources: Bug Downs Pay Phones, Today In New Zealand News, 10
Aug 2003, IRN,
and Payphone glitch toll known today, Philip English, 12 Aug
2003, New
Zealand Herald; PGN-ed]

<http://xtramsn.co.nz/news/0,,3882-2576232,00.html>

<http://www.nzherald.co.nz/storydisplay.cfm?storyID=3517597>

Free Software Foundation hacked

<Patrick Lincoln <lincoln@csl.sri.com>>

Sat, 16 Aug 2003 08:46:13 -0700

GNU Servers Hacked, Linux Software May Be Compromised, *Techweb News*

<http://www.internetwk.com/breakingNews/showArticle.jhtml?articleID=13100280>

In mid-March 2003, someone hacked the primary file servers hosted by the GNU Project, the group which supports the development of many of the components in the Linux operating system, the group acknowledged Wednesday. It warned that the attacker may have inserted malicious code into the free software available for download, including Linux, and posted a set of hashes that users can check against to determine if what they retrieved is clean. The CERT Coordination Center noted in an advisory posted on 13 Aug 2003 that "because this system serves as a centralized archive of popular software, the insertion of malicious code into the distributed software is a serious threat." At the same time, it reported that there isn't any evidence that the source code posted on the FTP servers was, in fact, compromised.

The Free Software Foundation (FSF), which oversees the GNU Project, has

posted a series of checksums, validation numbers generated by the source code known not to have been compromised, which users can use to verify what they've downloaded.

The attack took place in March, but was only discovered in late July. It used an exploit that was revealed on March 17, for which a patch wasn't immediately available. It was during a week's span of vulnerability that the servers were compromised, the FSF said in a statement.

A Trojan horse was placed on the system at that time, possibly for password collection and to use the machine for additional attacks, according to the FSF.

[See also <http://zdnet.com.com/2100-1105-5063658.html>

-- which prompted Keith Rhodes to note the following:

* The bad news: "The project urged those who have downloaded software

from the server since March to check that the source code has not been

tampered with."

* The good news: You actually have source you can check.

PGN]

🔥 Nasdaq reports incorrect pricing

<"Fuzzy Gorilla" <fuzzygorilla@euroseek.com>>

Fri, 15 Aug 2003 13:15:13 -0400

A computer glitch at Nasdaq evidently caused the network to report a false and exceedingly low trade price for Rentrak Inc. at the end of

trading on 13

Aug 2003. For a short time it was reported that common shares in Rentrak had closed at 15 cents, down nearly 98 percent from the previous close of \$6.65. The false price of 15 cents was in the data continuously supplied by Nasdaq to communication channels, such as wire services and web portals. A short time later the closing price was changed to \$6.28, down 5.6 percent from the previous day. [Source: Computer error sends Rentrak's reported stock price on roller coaster ride, Robert Goldfield, 13 Aug 2003, American City Business Journals Inc.; PGN-ed]

<http://portland.bizjournals.com/portland/stories/2003/08/11/daily33.html>

⚡ Legit website or nefarious scam?

<"Anderson, Matt" <manderson@gaic.com>>
Fri, 15 Aug 2003 16:52:16 -0400

I received an e-mail asking be to join something called the American Consumer Panel (<http://www.americanconsumerpanel.com>), and as a "perk" for joining, I would be sent an Amazon gift certificate. On the website, they claim to be a service of Forester Research (even links to Forester's site and shows a copyright (for what ever that is worth)) yet doing a search on Forester finds no mention of them. Anyways, something besides all of that made me suspicious (maybe how the URL got redirected to https://netpanel.gmi-mr.com/portals/gpms_cp/5000585/) so I

checked out the terms and conditions of membership and buried down in the middle of the terms was this gem,

"5. Third-Party Accounts

By participating in the Service, you authorize ACP to access your spending and savings in your personal accounts, including but not limited to your credit card and bank accounts, using ACP's secure, computerized system, [and authorize your third-party account providers to provide us with such information.] Where applicable, you also authorize ACP to record your Web-surfing behavior. You agree that ACP assumes no responsibility and shall incur no liability with respect to the acts, omissions, or determinations of any such third-party account providers."

Maybe it's over-reacting on my part, but ignoring the web-surfing monitoring, it seems a stretch for a research company to need to access my personal credit cards and bank accounts. Even if this is legitimate (I sent an e-mail to Forester and have not received a response), access is a very vague term. If I have access to something, what kind of permissions do I have? Can I remove money or transfer it to another account? Additionally, some banks charge you for 3rd party access so you could get whacked with all kinds of bank fees. Regardless, buried this deep into the terms and conditions makes this whole site very suspicious. Risks seem obvious enough...

M@ Anderson Sr. Enterprise Architect manderson@gaic.com

✶ easynet.nl is causing serious e-mail disruption

<Jim Garrison <jhg@acm.org>>

Sun, 17 Aug 2003 11:37:22 -0500

easynet.nl runs a SPAM blacklist based solely on source IP address and, as far as I can tell, uses a highly indiscriminate process for adding addresses that can be summarized as "One accusation and you're convicted" combined with "Guilty until proven innocent". Unfortunately, they are also one of the most widely used blacklists, and their popularity is threatening to seriously affect the ability to communicate by e-mail.

My hosting provider recently had to change its upstream provider and get new IP addresses because easynet had its entire class B netblock on the list to "punish" the owner of that netblock for perceived unwillingness or inability to police SPAM.

The new addresses come from class A block 69/8, which until fairly recently was unallocated. Somehow, the NEW address for my provider's SMTP server is also on easynet's list, so we're back where we started.

Easynet won't communicate with anyone about their decisions, and getting removed is nearly impossible. How long will it take before ISPs using easynet realize they're hurting their own subscribers as much as the spammers? This threatens to fragment the Internet into isolated islands

where large groups of users are unable to communicate with each other.

⚡ Re: Another variant on deceptive URLs (Brent, [RISKS-22.85](#))

<Dr John Stockton <spam@merlyn.demon.co.uk>>

Fri, 15 Aug 2003 22:00:24 +0100

>I can't be the first to point this out, but: having a character that is
>visually indistinguishable from the absence of a character is in itself a
>risk. Perhaps it would be useful for URL-display and similar outputs to use
>a visible character to indicate spaces, as can be done with word-processors?

The visible character might be misunderstood as representing itself.

Better to use a shading, or colour, to indicate non-character regions, IMHO.

Typically, text is black on white, for this, use whatever (20% black + 80% white) works out as, or similar. My site's URL would then display as

http://www.merlyn.demon.co.uk/#####...
where #####... represents light but unmistakable shading.

John Stockton, Surrey, UK. <URL:<http://www.merlyn.demon.co.uk/>>

⚡ Re: Identity Crisis and *The Washington Post* ([RISKS-22.84](#))

<Rob Slade <rslade@sprint.ca>>

Sat, 16 Aug 2003 12:36:31 -0800

> *The Washington Post Magazine* Cover Story:
> Identity Crisis, by Robert O'Harrow Jr.
> <http://www.washingtonpost.com/wp-dyn/articles/A25358-2003Aug6.html>

It is rather ironic, in view of the topic, that you cannot get to the story without allowing both cookies and JavaScript in your browser. The site itself sets about a dozen cookies on your machine, and there are outside sites that set cookies as well: something called surfaid (which I allowed), the ubiquitous Doubleclick (which I got away with blocking), and something called atdmt.com (which I allowed, out of fear that I wouldn't see the story otherwise).

rslade@vcn.bc.ca slade@victoria.tc.ca rslade@sun.soci.niu.edu
<http://victoria.tc.ca/techrev/~rslade> or <http://sun.soci.niu.edu/~rslade>

bardcode

<Jamie Zawinski <jwz@jwz.org>>
Fri, 15 Aug 2003 19:17:19 -0700

> [I somewhat reluctantly fixed a typo above: "bardcode" sounded
> appropriately Shakespearean for a library system. PGN]

Actually, Bardcode is a very cute Web site that presents the entire works of Shakespeare in barcode form.

<http://artcontext.net/bardcode/>

It seems to be down at the moment, but the Wayback Machine has it:

<http://web.archive.org/web/20020211011705/http://artcontext.net/bardcode/>



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 87

Thursday 21 August 2003

Contents

- [Nasty elevator death at Houston hospital](#)
- [Missing full-stop halts NZX trading](#)
[Gavin Treadgold](#)
- [Safe! until the 22st century?](#)
[Wendell Cochran](#)
- [Of course, it couldn't happen again!/The Road to Vulnerability](#)
[H.L.Hausen](#)
- [Tampa Police disband face-recognition software](#)
[PGN](#)
- [Botched 911 call led to man's death](#)
[Ben Moore](#)
- [Blackout: definitely not terrorists!](#)
[Martin Ward](#)
- [Robert X. Cringely on India, outsourcing, and IT productivity](#)
[PGN](#)
- [Lots of railroad traffic affected by so-big](#)
[Danny Burstein](#)
- [Increase in bounces from forgeries due to virus](#)
[PGN](#)
- [Sobig.F](#)

[Rob Slade](#)

● [Sobig side effects](#)

[Jim Griffith](#)

● [Firewall reject rates](#)

[Mike Hogsett](#)

● ["Good" Worm Fixes Infected Computers](#)

[Jim Schindler](#)

● [Send PIF files in ZIP attachment to avoid virus detectors?](#)

[Olivier Dagenais](#)

● [Do-Not-Spam list effort will be futile](#)

[NewsScan](#)

● [The Risks of Miniaturisation](#)

[Gene Wirchenko](#)

● [Update on NZ payphone failures](#)

[Don Mackie](#)

● [Out of context numbers: It wasn't quite THAT bad...](#)

[Andrew Greene](#)

● [Info on RISKS \(comp.risks\)](#)

⚡ Nasty elevator death at Houston hospital

<"Peter G. Neumann" <neumann@csl.sri.com>>

Mon, 18 Aug 2003 09:15:19 -0700 (PDT)

More for the "THIS CAN'T POSSIBLY HAPPEN" file:

Hitoshi Kikaidow, a surgical resident at Christus St. Joseph Hospital in Houston, was caught by a hospital elevator door as he stepped in, and was decapitated as the elevator ascended. A female hospital employee was in malfunctioning the elevator at the time, and was trapped until rescued by firefighters. Incidents with elevators and escalators kill about 30 people

and injure about 17,000 each year, according to the U.S. Bureau of Labor Statistics' Census of Fatal Occupational Injuries and more recent Consumer Product Safety Commission data. [PGN-ed from two sources]

Houston Chron:

<http://www.chron.com/cs/CDA/ssistory.mpl/metropolitan/2053346>

Newsday AP item:

<http://www.newsday.com/news/nationworld/wire/sns-ap-brf-doctor-decapitated,0,5206582.story?coll=sns-ap-nationworld-headlines>

And don't forget the "THIS CAN'T POSSIBLY HAPPEN AGAIN" file.

RISKS reported the earlier cases in Ottawa in which, following the first death in Apr 1989 ([RISKS-8.48,49,50,52,54](#)), a second death in Jun 1989 ([RISKS-8.77](#)) occurred; the known flaw in the 1954 Otis elevator door interlock logic causing the first death had remained uncorrected ([RISKS-9.01](#)). We also previously reported the Houston elevator that failed in the floods caused by Tropical Storm Allison and by default went down to the BOTTOM, drowning its occupant ([RISKS-21.47](#)). I recall another case in which elevator power failed because of a fire on the top floor, and the elevator by default went to the TOP floor, roasting its occupants, but I cannot find that case in our archives.

✶ Missing full-stop halts NZX trading

<"Gavin Treadgold" <gav@rediguana.co.nz>>

Thu, 21 Aug 2003 11:23:19 +1200

A missing full-stop in a piece of code for a trivial change to a software program reportedly started the chain of events that brought New Zealand's sharemarket to a halt yesterday.

<http://www.nzherald.co.nz/business/businessstorydisplay.cfm?storyID=3519114>

Computer glitch halts stock exchange trading

<http://www.stuff.co.nz/stuff/0,2106,2633746a13,00.html>

A faulty computer program at New Zealand's biggest share registrar halted trading on the stock exchange for more than five hours yesterday.

I guess that's got to be one of the smallest software bugs around :)

Safe! until the 22st century?

<Wendell Cochran <atrypa@eskimo.com>>

Tue, 19 Aug 2003 15:25:20 -0700

'Disaster Plans Get New Scrutiny After Blackout' runs a headline in **The New York Times**, 19 Aug 2003, C1. Alas, some company managers seem to evaluate risk in risky ways.

"Some customers learn from experience," reports John Schwartz of **The Times**, paraphrasing Don DeMarco, vice president for business continuity & recovery services at IBM, `but seem to learn the wrong lesson. He described a corporate client that survived a major flood with the help of

his
company's disaster recovery services, and then declined to renew
its
contract for the following year.

`Mr. DeMarco said he was aghast. "Are you kidding?" he recalled
asking.

"We just saved your company."

`The client, however, was unmoved. "We're in a hundred-year
flood zone,"

Mr. DeMarco recalled him saying, "and it just happened."

✶ Of course, it couldn't happen again!/The Road to Vulnerability

<"H.L.Hausen" <hausen@gmd.de>>

Mon, 18 Aug 2003 10:43:40 +0200

Some years ago I visited the Darlington PowerPlant in Ontario
and I was
surprised that the Power Grid Control System of the Niagara-
Mohawk power
grid did not include a "25% safety reserve" as usual. The
software engineers
there told me that the software has been proven to be safe and
reliable and
so that sort of traditional risk prevention was not necessary.
Is it that
sometimes software engineers don't like to listen to traditional
engineering
professionals? Wasn't there a problem with the Darlington
control software
some time ago? I assume a deeper investigation into the Grid
Control is
necessary.

[For previous RISKS items on Darlington, see [RISKS-9.64](#),
[11.08](#), [11.12](#),

[11.96](#), [12.49](#), [15.13](#), [15.59](#), [15.81](#), [17.47](#). PGN]

✶ Tampa Police disband face-recognition software

<"Peter G. Neumann" <neumann@csl.sri.com>>

Wed, 20 Aug 2003 09:47:51 -0500

The Tampa Police Department has eliminated the facial-recognition software hooked up to cameras scanning crowds in public places in Ybor City, after two years, with zero arrests and zero positive identifications, with a database of 30,000 mug shots of criminals and runaway children. [Source: *Tampa Tribune*, 20 Aug 2003]

<http://www.tampatribune.com/MGA0TF0TKJD.html>

✶ Botched 911 call led to man's death

<Ben Moore <ben.moore@juno.com>>

Sun, 17 Aug 2003 19:52:21 GMT

A 911 dispatcher in Buncome County, North Carolina, clicked on a box to transfer the house address of a caller into the Computer Aided Dispatch system. But that system, installed in March 2003, did not yet have information on all Buncombe County roads, and suggested an incorrect alternative (Briarcliff Drive, instead of Lane, in West Asheville), which the dispatcher accepted. As a result, the paramedics were significantly

delayed and the self-inflicted victim died. Attempts are now being made to complete the database. [Source: article by Tonya Maxwell, 15 Aug 2003, *Citizen-Times*; PGN-ed]
<http://cgi.citizen-times.com/cgi-bin/story/40174>

✶ Blackout: definitely not terrorists!

<Martin Ward <Martin.Ward@durham.ac.uk>>

Mon, 18 Aug 2003 10:29:45 +0100

Did anyone else notice this? All the early reports about the blackout said that they had **no** idea of the cause, or even in which country it originated (with Canada and the USA both pointing the finger at each other). But officials are absolutely certain that it was **not** caused by terrorist activity. Some reports were slightly more honest in saying that "we have no evidence of terrorist activity": not surprising since they had no evidence of **any** cause whatsoever. If "no evidence of terrorist activity" is the same as "definitely no terrorist activity", then the blackout definitely did not occur (because there is no evidence of **any** cause). Any actual loss of electricity you appear to observe is therefore merely the result of a deranged imagination...

Martin.Ward@durham.ac.uk <http://www.cse.dmu.ac.uk/~mward/>

✦ Robert X. Cringely on India, outsourcing, and IT productivity

<"Peter G. Neumann" <neumann@csl.sri.com>>

Sat, 16 Aug 2003 07:45:14 -0400

Those of you interested in problems associated with outsourcing might be interested in this article:

May the Source Be With You: IT Productivity Doesn't Have to Be an

Oxymoron, but Outsourcing Isn't the Way to Achieve It,
by Robert X. Cringely

<http://www.pbs.org/cringely/pulpit/pulpit20030814.html>

Cringely has a fascinating Web site. He also invites you at that URL to send this article to others, but I thought my including it in its entirety in a RISKS issue would be a little excessive, so I am merely posting the URL here.

✦ Lots of railroad traffic affected by so-big

<danny burstein <dannyb@panix.com>>

Wed, 20 Aug 2003 19:00:04 -0400 (EDT)

Computer Virus Strikes CSX Transportation Computers
Freight and Commuter Service Affected, 20 Aug 2003

CSX Transportation's (CSXT) information technology systems experienced significant slowdowns early today after a computer virus infected the network. The cause was believed to be a worm virus similar to

those that have infected the systems of other major companies and agencies in recent days. The infection resulted in a slowdown of major applications, including dispatching and signal systems. As a result, passenger and freight train traffic was halted immediately, including the morning commuter train service in the metropolitan Washington, D.C., area. Contrary to initial reports, the signal system for train operations was not the source of the problem. Rather, the virus disrupted the CSXT telecommunications network upon which certain systems rely, including signal, dispatching and other operating systems. [...]

http://www.csx.com/?fuseaction=company.news_detail&i=45722&news_year=-1

✶ Increase in bounces from forgeries due to virus

<"Peter G. Neumann" <neumann@csl.sri.com>>

Tue, 19 Aug 2003 14:49:35 PDT

Incidentally, the number of bounces from messages sent with forged FROM: addresses (appearing to come from me and various others of you who are remarking thereupon) seems to have taken a huge quantum leap in the past few days. I'm suddenly getting even more bounces than usual, due to the new W32.Sobig.F virus. My regrets if you are getting any such forged e-mail. However, it is not coming from my mailer, because I do not use **any** Microsoft software. Just look at the last RECEIVED: line

(unless your
stupid mailer hides it!).

Typical subject lines include these:

Re: Details
Re: Approved
Re: Re: My details
Re: Thank you!
Re: That movie
Re: Wicked screensaver
Re: Your application
Thank you!
Your details

and attachments such as:

application.zip
details.zip
document_....zip
movie....zip
thank_you.zip
your_details.zip
your_document.zip
wicked_scr.zip

You can read more about this virus online at:

<http://securityresponse.symantec.com/avcenter/venc/data/w32.sobig.f@mm.html>

Sobig.F

<Rob Slade <rslade@sprint.ca>>
Thu, 21 Aug 2003 11:05:42 -0800

Sobig load is increasing: over the past 15 hours I've received 52 copies in my inbox, up from yesterday's 47 in 20 hours (and, as previously noted, well exceeding the previous record for Klez at its height). (On the slightly

bright side, spammers seem to have been affected: other spam seems slightly down today :-)

As noted, Sobig uses its own SMTP engine, and spoofs both the From and Return-Path headers on a random basis, so that is no indication. However, the message body is always "Please see the attached file for details." so that is a reliable indicator. In addition, I've had a look at more headers, and the following two seem to appear in every copy I've received:

```
X-MailScanner: Found to be clean
X-Mailer: Microsoft Outlook Express 6.00.2600.0000
```

PLEASE spread the word: DO NOT OPEN ATTACHMENTS. If in doubt, don't.

Sobig uses no special technology beyond this rather simplistic social engineering. (Can anyone tell me: is there any content scanner lazy enough to be bypassed by the X-MailScanner header?)

<http://www.sophos.com/virusinfo/analyses/w32sobigf.html>

http://www.f-secure.com/v-descs/sobig_f.shtml

rslade@vcn.bc.ca slade@victoria.tc.ca rslade@sun.soci.niu.edu

<http://victoria.tc.ca/techrev> or <http://sun.soci.niu.edu/~rslade>

⚡ Sobig side effects

<griffith@dweeb.org (Jim Griffith)>

Thu, 21 Aug 2003 13:57:21 -0500

Unlike Blaster and other past worms and viruses, the rec.humor.funny moderating addresses have been hammered by the Sobig worm. In the past 48 hours, I've seen some 3500 worm-related e-mail messages sent to the three or four moderating addresses that I use, resulting in a DOS of e-mail and submission processing. As this worm does the "send the worm out as if from someone else" trick, and as the RHF addresses have been around for years, the worm is apparently masquerading as coming from me in a lot of instances, despite the fact that the RHF machines run LINUX and are immune to it. So a fair number of the worm-related pieces of e-mail are mail bounces and quarantine messages generated by other sites' anti-virus software.

Most annoying is that some of the addresses targeted by the worm are mailing list subscription addresses. While many of them are smart enough to either look for keywords like SUBSCRIBE or require confirmation, some of them are not. As a result, I find that the RHF-related addresses are now subscribed to mailing lists devoted to jokes, religious and political topics, and one which discusses issues important to Raelians. I've also found that I've apparently opened customer support tickets with any number of companies as well.

It's disappointing that despite the surge in e-mail viruses in past years, many systems still allow actions to be triggered by a single e-mail, with no outside confirmation required.

🔥 Firewall reject rates

<Mike Hogsett <hogsett@csl.sri.com>>

Tue, 19 Aug 2003 14:07:14 -0700

The following are the file sizes for our compressed daily firewall logs.

There are a few interesting dates. The spike for 26 Jan 2003 is the SQL

Slammer worm. The increase in early March is an exploit for port 445 on MS

products. Finally the major spike on Aug 12 is Blaster.

So, we have gone from about 2Mbytes/day of compressed log data at the

beginning of the year to about 20Mbytes/day now. There is no end in sight.

[There is no site to end. PGN]

1-Jan-2003	2M	**
2-Jan-2003	2M	**
3-Jan-2003	2M	**
4-Jan-2003	3M	***
5-Jan-2003	1M	*
6-Jan-2003	2M	**
7-Jan-2003	2M	**
8-Jan-2003	3M	***
9-Jan-2003	3M	***
10-Jan-2003	3M	***
11-Jan-2003	3M	***
12-Jan-2003	3M	***
13-Jan-2003	3M	***
14-Jan-2003	3M	***
15-Jan-2003	3M	***
16-Jan-2003	3M	***
17-Jan-2003	2M	**
18-Jan-2003	3M	***
19-Jan-2003	3M	***

20-Jan-2003	3M	***
21-Jan-2003	2M	**
22-Jan-2003	2M	**
23-Jan-2003	3M	***
24-Jan-2003	3M	***
25-Jan-2003	9M	*****
26-Jan-2003	24M	*****
27-Jan-2003	8M	*****
28-Jan-2003	5M	*****
29-Jan-2003	4M	****
30-Jan-2003	3M	***
31-Jan-2003	2M	**
1-Feb-2003	3M	***
2-Feb-2003	3M	***
3-Feb-2003	2M	**
4-Feb-2003	3M	***
5-Feb-2003	2M	**
6-Feb-2003	3M	***
7-Feb-2003	3M	***
8-Feb-2003	4M	****
9-Feb-2003	3M	***
10-Feb-2003	4M	****
11-Feb-2003	3M	***
12-Feb-2003	3M	***
13-Feb-2003	3M	***
14-Feb-2003	3M	***
15-Feb-2003	3M	***
16-Feb-2003	3M	***
17-Feb-2003	3M	***
18-Feb-2003	3M	***
19-Feb-2003	3M	***
20-Feb-2003	3M	***
21-Feb-2003	2M	**
22-Feb-2003	3M	***
23-Feb-2003	3M	***
24-Feb-2003	3M	***
25-Feb-2003	3M	***
26-Feb-2003	4M	****
27-Feb-2003	3M	***
28-Feb-2003	3M	***
1-Mar-2003	3M	***
2-Mar-2003	2M	**
3-Mar-2003	3M	***

4-Mar-2003	4M	****
5-Mar-2003	4M	****
6-Mar-2003	4M	****
7-Mar-2003	5M	*****
8-Mar-2003	6M	*****
9-Mar-2003	11M	*****
10-Mar-2003	12M	*****
11-Mar-2003	11M	*****
12-Mar-2003	10M	*****
13-Mar-2003	11M	*****
14-Mar-2003	12M	*****
15-Mar-2003	10M	*****
16-Mar-2003	10M	*****
17-Mar-2003	9M	*****
18-Mar-2003	9M	*****
19-Mar-2003	10M	*****
20-Mar-2003	11M	*****
21-Mar-2003	12M	*****
22-Mar-2003	10M	*****
23-Mar-2003	11M	*****
24-Mar-2003	6M	*****
25-Mar-2003	10M	*****
26-Mar-2003	10M	*****
27-Mar-2003	10M	*****
28-Mar-2003	12M	*****
29-Mar-2003	11M	*****
30-Mar-2003	10M	*****
31-Mar-2003	9M	*****
1-Apr-2003	12M	*****
2-Apr-2003	13M	*****
3-Apr-2003	11M	*****
4-Apr-2003	10M	*****
5-Apr-2003	10M	*****
6-Apr-2003	13M	*****
7-Apr-2003	9M	*****
8-Apr-2003	11M	*****
9-Apr-2003	11M	*****
10-Apr-2003	11M	*****
11-Apr-2003	11M	*****
12-Apr-2003	12M	*****
13-Apr-2003	12M	*****
14-Apr-2003	11M	*****
15-Apr-2003	12M	*****

16-Apr-2003	12M	*****
17-Apr-2003	10M	*****
18-Apr-2003	11M	*****
19-Apr-2003	11M	*****
20-Apr-2003	10M	*****
21-Apr-2003	10M	*****
22-Apr-2003	11M	*****
23-Apr-2003	13M	*****
24-Apr-2003	13M	*****
25-Apr-2003	13M	*****
26-Apr-2003	12M	*****
27-Apr-2003	10M	*****
28-Apr-2003	11M	*****
29-Apr-2003	15M	*****
30-Apr-2003	11M	*****
1-May-2003	11M	*****
2-May-2003	10M	*****
3-May-2003	11M	*****
4-May-2003	10M	*****
5-May-2003	9M	*****
6-May-2003	12M	*****
7-May-2003	11M	*****
8-May-2003	10M	*****
9-May-2003	9M	*****
10-May-2003	10M	*****
11-May-2003	9M	*****
12-May-2003	9M	*****
13-May-2003	13M	*****
14-May-2003	10M	*****
15-May-2003	10M	*****
16-May-2003	10M	*****
17-May-2003	11M	*****
18-May-2003	9M	*****
19-May-2003	10M	*****
20-May-2003	10M	*****
21-May-2003	11M	*****
22-May-2003	9M	*****
23-May-2003	10M	*****
24-May-2003	12M	*****
25-May-2003	10M	*****
26-May-2003	11M	*****
27-May-2003	10M	*****
28-May-2003	13M	*****

29-May-2003	10M	*****
30-May-2003	11M	*****
31-May-2003	10M	*****
1-Jun-2003	7M	*****
2-Jun-2003	8M	*****
3-Jun-2003	11M	*****
4-Jun-2003	10M	*****
5-Jun-2003	11M	*****
6-Jun-2003	10M	*****
7-Jun-2003	12M	*****
8-Jun-2003	12M	*****
9-Jun-2003	12M	*****
10-Jun-2003	14M	*****
11-Jun-2003	12M	*****
12-Jun-2003	13M	*****
13-Jun-2003	10M	*****
14-Jun-2003	11M	*****
15-Jun-2003	9M	*****
16-Jun-2003	10M	*****
17-Jun-2003	14M	*****
18-Jun-2003	13M	*****
19-Jun-2003	13M	*****
20-Jun-2003	11M	*****
21-Jun-2003	11M	*****
22-Jun-2003	9M	*****
23-Jun-2003	9M	*****
24-Jun-2003	11M	*****
25-Jun-2003	12M	*****
26-Jun-2003	10M	*****
27-Jun-2003	12M	*****
28-Jun-2003	14M	*****
29-Jun-2003	11M	*****
30-Jun-2003	10M	*****
1-Jul-2003	14M	*****
2-Jul-2003	9M	*****
3-Jul-2003	10M	*****
4-Jul-2003	11M	*****
5-Jul-2003	11M	*****
6-Jul-2003	8M	*****
7-Jul-2003	9M	*****
8-Jul-2003	14M	*****
9-Jul-2003	10M	*****
10-Jul-2003	8M	*****

11-Jul-2003	9M	*****
12-Jul-2003	10M	*****
13-Jul-2003	7M	*****
14-Jul-2003	8M	*****
15-Jul-2003	12M	*****
16-Jul-2003	10M	*****
17-Jul-2003	9M	*****
18-Jul-2003	10M	*****
19-Jul-2003	8M	*****
20-Jul-2003	9M	*****
21-Jul-2003	8M	*****
22-Jul-2003	11M	*****
23-Jul-2003	9M	*****
24-Jul-2003	8M	*****
25-Jul-2003	9M	*****
26-Jul-2003	8M	*****
27-Jul-2003	8M	*****
28-Jul-2003	7M	*****
29-Jul-2003	12M	*****
30-Jul-2003	9M	*****
31-Jul-2003	9M	*****
1-Aug-2003	9M	*****
2-Aug-2003	8M	*****
3-Aug-2003	7M	*****
4-Aug-2003	7M	*****
5-Aug-2003	11M	*****
6-Aug-2003	8M	*****
7-Aug-2003	7M	*****
8-Aug-2003	8M	*****
9-Aug-2003	6M	*****
10-Aug-2003	7M	*****
11-Aug-2003	7M	*****
12-Aug-2003	44M	*****
13-Aug-2003	35M	*****
14-Aug-2003	24M	*****
15-Aug-2003	20M	*****
16-Aug-2003	15M	*****
17-Aug-2003	11M	*****
18-Aug-2003	12M	*****
19-Aug-2003	26M	*****

✶ "Good" Worm Fixes Infected Computers

<Jim Schindler <Jimschin@pacbell.net>>

Mon, 18 Aug 2003 20:10:24 -0700

A new Internet worm emerged today that is designed to seek out and fix any computer that remains vulnerable to "Blaster," the worm that attacked more than 500,000 computers worldwide last week. The new worm scours the Internet for computers already infected with Blaster and deletes the "bad" worm, according to two anti-virus software vendors. The worm then fixes the computers with one of eight software patches developed by Microsoft Corp, and it uses infected computers as a base for searching the Internet for other vulnerable systems. Blaster and the new worm both target vulnerabilities in recent versions of Windows XP, Windows 2000 and Windows NT 4.0. Even though the new worm is "good," it can cause plenty of trouble for computer users ... Buried within the code of the new worm is the message: "I love my wife & baby :-) ~ ~ Welcome Chian ~ ~ Notice: 2004 will remove myself:-) ~ ~ sorry." [From the titled article by Brian Krebs, *The Washington Post*, 18 Aug 2003]

✶ Send PIF files in ZIP attachment to avoid virus detectors?

<"Olivier Dagenais" <olivier_dagenais@canada.com>>

Wed, 20 Aug 2003 21:52:15 -0400

With the recent rebirth of the Sobig virus/worm, I have found myself on the receiving end of many messages being bounced back, saying I reached accounts that do not exist, are over quota or that do not allow certain attachments to come through, such as in the following response:

This message has been rejected because it has a potentially executable attachment "thank_you.pif" This form of attachment has been used by recent viruses or other malware. If you meant to send this file then please package it up as a zip file and resend it.

The RISKS? How long until a virus sends itself in a ZIP file attachment, thereby bypassing traditional virus detection routines and people implicitly trusting said attachments and their contents? (doesn't most ZIP software make ZIPs transparent to the users, anyway?)

Oh, and did I mention that the bounced message also included said "potentially executable attachment"? What a great virus re-distribution mechanism!

(IIRC) PIF files were the precursors to shortcuts and never were meant to contain executable code, so why EVER trust them as executable code? (although banning them is a risk in itself, if some unfortunate soul were to write a program to manage, say, personal information files...)

⚡ Do-Not-Spam list effort will be futile

<"NewsScan" <newsscan@newsscan.com>>

Wed, 20 Aug 2003 09:16:15 -0700

Federal Trade Commission Chairman Timothy Muris says that even if efforts in Congress to establish a "do-not-spam" list succeed, that won't fix the problem of unwanted junk mail. "If such a list were established, I'd advise customers not to waste their time and effort. Most spam is already so clearly illegitimate that the senders are no more likely to comply with new regulations than with the laws they now ignore." The drive toward setting up a "do-not-spam" list has picked up steam following the popularity of the FTC's recently established "do-not-call" registry for people who want to stop telemarketing calls. Muris says the magnitude of the problem and the fact that "spammers can easily hide their identities and cross international borders," makes government regulation extremely difficult. "In the end, spam will be reduced, if at all, through several technological improvements, as well as safer computing practices by others." [AP 19 Aug 2003; NewsScan Daily, 20 August 2003]

<http://apnews.excite.com/article/20030819/D7T1A63G3.html>

✶ The Risks of Miniaturisation

<Gene Wirchenko <genew@mail.ocis.net>>

Sun, 17 Aug 2003 12:30:24 -0700

I recently lost some very useful data. It was on a USB memory stick. As far as I can tell, I forgot to remove the itty-bitty memory stick before leaving a college workstation. I did get the memory stick back, but it occurred to me how very unlikely I would be to forget with something bigger. I now attach the memory stick to my pants with the cord that came with it.

✶ Update on NZ payphone failures ([RISKS-22.86](#))

<Don Mackie <donald@iconz.co.nz>>

Tue, 19 Aug 03 21:42:04 +1200

Some more details in the story at:

<http://www.nzherald.co.nz/storydisplay.cfm?storyID=3518759&thesection=business&thesubsection=technology>

I had never heard of The Centre for Critical Infrastructure Protection before. I work in health and am involved in some disaster preparedness committees. Probably my own fault for not asking. They seem to be more interested in information systems infrastructure than water/power.

Don Mackie <www.ccip.govt.nz>

[Error in Subject line in [RISKS-22.86](#) is corrected in archives. PGN]

✶ Out of context numbers: It wasn't quite THAT bad...

<agreene@pageflexinc.com (Andrew Greene)>

Wed, 20 Aug 2003 12:54:48 -0400

PGN's summary in [RISKS-22.85](#) included the sentence: "At least 50 million people were affected." But according to *The New York Times* ("How Many in the Dark? Evidently Not 50 Million" by Mike McIntire, 17 Aug 2003, currently at <http://www.nytimes.com/2003/08/17/nyregion/17NUMB.html>), that number was actually the total population of the overall geographical areas served by utility companies that were affected, and could be taken as a hard upper limit on the number of customers affected. However, the number was lifted out of context and then got exaggerated by politicians and news reporters looking to make a big story sound even more impressive:

"Approximately 61,800 megawatts of customer load was lost in an area that covers 50 million people. ... We cannot say with precision how many customers were affected at this time." [...] For instance, in the New York region, where approximately 18 million people live, nearly 20 percent of the available electricity remained on, according to the New York Independent System Operator, which monitors electrical usage.

[Andrew, Just because someone was not out of power does not mean that person was not affected. But you are quite correct. The quoted 50 million number was erroneously qualified. TNX. PGN]



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

[ACM](#) Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 88

Wednesday 27 August 2003

Contents

- [California accepts completely unverified updates](#)
[Geoff Kuenning](#)
- [BlackBerry reveals sensitive Morgan Stanley data](#)
[Mark Feit](#)
- [Cingular wants me to pay negative balance](#)
[Ulf Lindqvist](#)
- ['Entrepreneur' a trademarked word, court rules](#)
[Christine Van Dusen via Monty Solomon](#)
- [Slammer worm hits system within Davis-Besse nuclear power plant](#)
[Fuzzy Gorilla](#)
- [Sobig affects Amtrak trains, Air Canada](#)
[Marty Leisner](#)
- [Some observations on e-mail phenomenology](#)
[Peter B. Ladkin](#)
- [Update on Sobig stage 2](#)
[Rob Slade](#)
- [Thank you for \[...\]](#)
[Rob Slade](#)
- [Organized crime behind Sobig mess?](#)
[NewsScan](#)

- [Re: Send PIF files in ZIP attachment to avoid virus detectors?](#)
[Robert de Bath](#)
 - [Re: Pilot fixes faulty jet](#)
[Peter B. Ladkin](#)
 - [Satellite photo of Eastern North America during blackout](#)
[John Oram](#)
 - [2004 IEEE Symposium on Security and Privacy, Call for Papers](#)
[David Wagner](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✂ California accepts completely unverified updates

<<geoff@cs.hmc.edu>>

Mon, 25 Aug 2003 16:52:57 -0700 (PDT)

I own a tiny California corporation for consulting purposes. Each year, I am required to file a "statement by domestic stock corporation" with information such as my address and the names of corporate officers.

This year, it is possible file electronically (a necessity for me because the state reverted to a 5-year-old address, which is another story of incompetence). The Web form tends to crash browsers, but I eventually succeeded with Mozilla. You type in the name of the corporation, fill out the forms, and pay your \$25 via credit card.

All of this is done with NO VERIFICATION WHATSOEVER. If I had a stolen credit card, I could change the addresses and officers of Microsoft, Bank of America, and a zillion other corporations. Straightening out the mess would

probably cost the state far more than the \$25 per instance that they wouldn't be able to collect from the credit card company anyway.

Geoff Kuenning geoff@cs.hmc.edu <http://www.cs.hmc.edu/~geoff/>

✶ BlackBerry reveals sensitive Morgan Stanley data

<Mark Feit <mfeit@notonthe.net>>

Tue, 26 Aug 2003 09:23:37 -0400

We've seen this before with hard disks. The article goes on to point out that this has started to happen more frequently as people are synchronizing their mobile devices with their desktops.

The eBay ad read "BlackBerry RIM sold AS IS!" So Eugene Sacks (not his

real name), a Seattle computer consultant who always wanted one of the

pager-size devices to check his e-mail, sent in a bid. For just \$15.50, he

bought the wireless device with 4 MB of memory. The BlackBerry didn't

come with a cable, synching station, software or a manual. But it did come

with something even more valuable: a trove of corporate data.

<http://www.wired.com/news/print/0,1294,60052,00.html>

✶ Cingular wants me to pay negative balance

<Ulf Lindqvist <ulf@sdl.sri.com>>

Fri, 22 Aug 2003 21:24:07 -0700 (PDT)

This item seems tragically funny. I canceled my service from Cingular Wireless some months ago, and in the final bill it turned out that I had paid \$3.36 too much. After some time they sent me a check, which I cashed. After another couple of weeks, I received the e-mail below. I hope they keep charging late fees for a negative balance, and I hope the fees will be negative too!

> Dear ULF LINDQVIST,
>
> Your current Cingular Wireless statement for account number [...] is
> now available for viewing on the Cingular Web Site at
> <https://myaccount.cingular.com>. The statement amount of \$-3.36 is due and
> payable immediately. A late fee will be assessed after 07/28/2003.

Also note that the message was sent on 08/22/2003...

'Entrepreneur' a trademarked word, court rules

<Monty Solomon <monty@roscom.com>>

Mon, 25 Aug 2003 09:48:11 -0400

Be careful if you use the word "entrepreneur." You might get sued.

Christine Van Dusen, *The Atlanta Journal-Constitution*, 25 Aug 2003

A federal judge recently ruled that the owner of Entrepreneur Magazine, a small-business publication with about 2 million readers nationwide, has dibs

on the term. Entrepreneur Media, based in California, trademarked the word after starting its magazine in 1978. And that, according to the court's decision, means the firm has "exclusive right to use the mark in commerce."

<http://www.ajc.com/business/content/business/0803/20entrepreneur.html>

Slammer worm hits system within Davis-Besse nuclear power plant

<"Fuzzy Gorilla" <fuzzygorilla@euroseek.com>>

Fri, 22 Aug 2003 17:53:25 -0400

The Register (and other sites) are reporting that a PC associated with the safety monitoring system at Davis-Besse nuclear power plant in Ohio.

This happened in January 2003, and there was no safety hazard because the plant was offline and "the monitoring system, called a Safety Parameter Display System, had a redundant analog backup that was unaffected by the worm" but helps to illustrate the risks of having "a crunchy shell around a soft, chewy center."

The plant had a firewall but...

"The Slammer worm entered the Davis-Besse plant through a circuitous route. It began by penetrating the unsecured network of an unnamed Davis-Besse contractor, then squirmed through a T1 line bridging that network and

Davis-Besse's corporate network. The T1 line, investigators later found, was one of multiple ingresses into Davis-Besse's business network that completely bypassed the plant's firewall, which was programmed to block the port Slammer used to spread."

<http://www.theregister.co.uk/content/56/32425.html>

[H. Ludwig Hausen noted this as well:
<http://www.securityfocus.com/news/6767>]

☛ Sobig affects Amtrak trains, Air Canada

<Marty Leisner <leisner@rochester.rr.com>>

Sat, 23 Aug 2003 13:36:34 -0400

Read about the impacts of Sobig on Amtrak and Air Canada!!

In the **Wall Street Journal**, 21 Aug 2003, there was an article "Computer Viruses Disrupt Railroad and Air Traffic"

It said: "A variant of the Blaster virus on Tuesday affected about half of Air Canada's phone-reservation capacity and some of its airport check-in operations, said spokesman John Rebel. In general, the virus simply slowed the process of taking reservations, but in a small number of cases, the problems caused flights to be delayed or canceled altogether, he said. Service was returned to normal by Wednesday."

It also said: "Dan Murphy, a spokesman for CSX, said the company noticed Wednesday at about 1:15 a.m. that a variant of the Blaster virus

was interfering with its train operations and dispatching system. The company curtailed rail service throughout the CSX network while its technicians tried to fix the problem. CSX operates about 1,600 freight, Amtrak and commuter trains a day on its 23,000-mile route network east of the Mississippi River."

The first case I just consider business stupidity -- the second case I consider much more serious -- it affected the signaling on rails. I find it hard to understand why general purpose computers are used in such specialized applications -- and ones that are easily compromised. I have to wonder what the requirements for these systems are (assuming they have requirements!!)

[Air Canada case also noted by Amos Shapir and Fuzzy Gorilla. PGN]

✶ Some observations on e-mail phenomenology

<"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>>
Wed, 27 Aug 2003 11:48:22 +0200

I have seen many technical proposals arising from the changing phenomenology of e-mail (e.g., Garfinkel, Anti-spam technology, [RISKS-19.24](#), Tripoli in [RISKS-22.83](#)), and increasingly many political proposals (e.g., Lincoln, [RISKS-22.86](#)). In order to evaluate the social worth of any of these, it is

necessary to understand the changing phenomenology of e-mail, just as political scientists must base their analyses and projections on concrete data. In contrast to technical and political proposals, I have seen relatively few public comments on the phenomenology (qualitative assessment) and phenomenography (quantitative assessment) of e-mail traffic.

A look at the RISKS archives may serve as a sample. Peter Neumann was already talking about the situation being "out of hand" six years ago (a June 1997 example of phenomenology in his editorial comment on Garfinkel, [RISKS-19.24](#)). Mike Hogsett's recent server data ([RISKS-22.87](#)) contributes to the phenomenography.

As others have remarked, e-mail traffic has markedly increased in recent weeks, due apparently to proliferation of the Sobig virus and the e-mail it generates. It seems certain that significant changes will be made at many organisations because of it. Some phenomenological comments are in order.

Like many contributors to RISKS, I have been using e-mail as a major professional tool for twenty years, and have been running my own server for the last nine. In this time, we have made three substantial technical changes. Two of those were to accommodate client facilities, namely a change to POP to accommodate portables, and a change to IMAP to accommodate PDAs + mobile phones.

Until recently, I accommodated the changing phenomenology of e-mail by

changing my working practices. However, our third major change, just over a year ago, was the introduction of heavy filtering, because the level of spam and resulting cost in time and connect charges precluded continued use of my Nokia Communicator to read e-mail on the road.

Sobig is something else. We are a Unix/Linux shop, so we don't contribute ourselves to the proliferation. The phenomenon will cause us to make changes, but because of the observations that follow, it is not clear yet what they will be.

My personal e-mail traffic has increased by up to an order of magnitude in the last weeks. My wanted e-mail has been 2-5% of the total, contrasted with the previous (estimated) 20%. All of the increase is unwanted mail generated by Sobig. The surprise is how it has been generated. The extra traffic is of five kinds:

1. Instances of Sobig-generated e-mail;
2. Bounce messages from e-mail servers unable to deliver an instance of a Sobig-generated mail and which reply to the address on the From header line;
3. Bounce messages from e-mail servers which have detected instances of Sobig with my e-mail address on the From header line;
4. Sobig-generated messages whose contents have been modified by our university computer center filter;
5. Personal inquiries by genuine correspondents who have received a message of type 3 with my e-mail address on the From header line.

We don't filter for Sobig. We haven't needed to - I can accommcoodate messages of type 1 under my normal working practice (a guarded thank you

to everybody else!). Servers generating messages of type 2 don't filter, either. Messages of types 3 and 4 are causing the most traffic, and the greatest difficulty.

The general phenomenology of Sobig-generated e-mails has been known for a while. Relevant are

- i. The e-mails, header and content, are entirely automatically generated; there is no piggy-backing on genuine e-mail;
- ii. The sender address is falsified, and ultimately derived from address-book entries on some infected machine;
- iii. There are technically easily-recognisable distinguishing syntactic features of these virally-generated e-mails.

Effective counters (programs which recognise the features in iii) have been known for a while, and details have been published in sources of record for at least a week, e.g., in German, <http://www.heise.de/security/news/meldung/39589>

Because of feature i, there is no disadvantage to anyone if a server deletes Sobig-generated e-mails. Because of feature ii, there is neither advantage nor necessity in informing either falsified "sender" or receiver. I would have thought that these observations would have been obvious to any system administrator.

But if they were uniformly (rationally) acted on, I would be receiving no mails of types 3 and 4, whereas mails of these types are causing me by far the biggest problem. If this observation generalises, then the major problem would appear to be generated not by the virus itself, but by the reactions of e-mail-server administrators.

I would have thought that e-mail service providers would be motivated to minimise the traffic generated by malware. This is apparently not so. Major ISPs such as AOL have been responsible for many messages of type 3.

I conclude that some work needs to be done to attempt to understand the organisational motivations and behavior of system administration, and to devise ways of preventing the collective behavior of professional administrators from making problems a lot worse than they otherwise would be.

Peter B. Ladkin, University of Bielefeld, Germany
<http://www.rvs.uni-bielefeld.de>

✶ Update on Sobig stage 2

<Rob Slade <rslade@sprint.ca>>
Fri, 22 Aug 2003 13:08:18 -0800

About 4 hours before it was due to trigger, F-Secure found an encrypted section of code in the Sobig virus that indicated an unsuspected payload.

At 1900H UTC (noon, PDT) on Friday, infected computers would try to connect to a number of servers, download a program, and run it.

Within that four hour period, F-Secure, possibly with the assistance of other institutions, was able to contact the ISPs for these machines, and have them all shut down. (One remains up. Presumably it has been turned into a honeypot, a form of trap for the people who intended to use it for the attack.)

At this time, we do not know what the intention of the so-called "Stage 2" payload was, but the plan shows evidence of very careful

planning, and,
given the extreme number of Sobig infections, it could have been
very
serious.

http://www.f-secure.com/news/items/news_2003082200.shtml

http://www.f-secure.com/v-descs/sobig_f.shtml

rslade@vcn.bc.ca slade@victoria.tc.ca rslade@sun.soci.
niu.edu

<http://victoria.tc.ca/techrev> or [http://sun.soci.niu.edu/
~rslade](http://sun.soci.niu.edu/~rslade)

✶ Thank you for [...]

<Rob Slade <rslade@sprint.ca>>

Mon, 25 Aug 2003 13:01:06 -0800

Thank you for the details about that movie regarding my
application for
the approved wicked screensaver!

Given that Sobig.F seems to have subsided from its weekend peak
(from my
numbers, it was doubling every day last week up until Sunday and
then
suddenly dropped off--to a rate that is still roughly as high as
Klez at its
worst) and that "Stage 2" seems to have been averted, a few
thoughts.

Blaster, a worm, infected relatively few machines but
inconvenienced (and in
some cases worse) companies, so it gets it's name in the paper.
Sobig
surpasses all records in terms of number of e-mail messages
generated, and
almost nobody (outside of our little security circle) is paying

attention.

Spoofing of e-mail headers in virus messages goes back to Hybris or before.

Most of the successful e-mail viruses have used some form of spoofing. Yet antivirus companies, in their mail server based products, are continuing to generate bounce messages to the nominal sender, probably in an attempt to market their products.

I got a lot of bounced Sobig over the past week. None, of course, had been sent from me. What these bounces are actually doing is aiding the virus: the bounce messages send the virus (a full copy of the original message is often included) to yet another machine. Spammers have also been using spoofed e-mail addresses for some time. Bounced spam is therefore also helping spammers to spread their messages. Two spam for the price of one, thanks to bounces. (Occasionally I hear of a server being inundated by a faked sender address on spam, but this seems to be rare. Which would seem to indicate that spammers are deliberately using random addresses, possibly for reasons of multiplication through bounces.)

One of the interesting points to come out the height of the Sobig numbers on Saturday, was that I saw relatively *few* bounces, in proportion to what one might have thought was the case. My address is obviously on enough infected machines for me to get huge numbers of infected messages: due to the way the virus spoofs addresses, a large number of the Sobig messages would have been sent "from" me. Given that the majority of server based

antiviral packages
do bounce messages, the penetration of server based virus
scanning would
therefore seem to be quite low. (Interesting, the indirect
things you can
learn in the aftermath of an attack. Consider the subject line
of this
message a test of content scanners still doing simplistic
subject line
rejections.)

I have been warning about the type of convergence of malware
technologies
involved in the "stage 2" situation for a few years now. Will
it be taken
seriously after Sobig? (Listen to the sound of me *not* holding
my breath.)
Sobig seems to have been planned and designed with much greater
care than is
usually the case with viruses and malware. Up until now, we
have been
spared what viruses *could* do primarily by the fact that we
have been
facing a bunch of disorganized amateurs. A number of comments
about Sobig
have raised the possibility of an involvement with spammers and/
or organized
crime. (We already know that "red guest" groups in China are
much more
organized and disciplined than traditional blackhats.) Sobig
may simply be
the result of an isolated creative mind, but relying on that
supposition as
fact is dangerous security planning.

Buried in the investigations into Sobig.F, you will find
reference to the
fact that it stops reproducing after September 10th. I'm afraid
it took my
wife pointing it out to make me realize that this is one day
before
September 11th. Sobig.G, anyone?

rslade@vcn.bc.ca
niu.edu

slade@victoria.tc.ca

rslade@sun.soci.

[http://victoria.tc.ca/techrev
~rslade](http://victoria.tc.ca/techrev~rslade)

or

<http://sun.soci.niu.edu/>

✶ Organized crime behind Sobig mess?

<"NewsScan" <newsscan@newsscan.com>>

Tue, 26 Aug 2003 08:28:20 -0700

Antivirus specialist Peter Simpson warns that the Sobig.F virus is the latest in a series of attempts on the part of organized crime to shift some of their illicit activities online. "Sobig smashed all the records in terms of pure numbers, but that's not nearly the whole story. This is the sixth in a series of controlled experiments. This isn't about some kiddy writing viruses in his bedroom -- this is really a very sophisticated example of organized crime," says Simpson, a manager at Clearswift's ThreatLab. Simpson explained that the purpose of a virus such as Sobig isn't to cause damage, but to gain control of the machine in order to access information such as financial details for the purpose of fraud. It also comes in handy for disguising the source of spam by hijacking the victim's machine and identity. "The real question here has to be about the motives of the virus writer. This isn't just about writing a virus that will spread rapidly and break records; the motives here are very different and are clearly

criminal. It's all about the hidden agenda." [ZDNet/Silicon.com
25 Aug
2003; NewsScan Daily, 26 August 2003]
http://zdnet.com.com/2100-1105_2-5067494.html

⚡ Re: Send PIF files in ZIP attachment to avoid virus detectors?

<Robert de Bath <robert\$@mayday.cix.co.uk>>
Sat, 23 Aug 2003 08:00:26 +0100 (BST)

> How long until a virus sends itself in a ZIP file attachment
[...]

Already done, I recently had a copy of 'W32/Mimail.A@mm' on the
15th in my
linux mailbox (virus are normally filtered like other junk) and
it's even
worse than you think.

The outer message was from the sysadmin of `_my_` domain, there
was a zip that
contained an html file. The html file was a mis-labeled file
containing a
MIME content type at the start and a PE executable at the end so
IE would
(presumably) run the executable ...

Hmm, I need to check that my "html cleaner" will (at least!)
break one
of those files.

PIFs are some weird windows hack yes, as for file extensions,
personally
I always do a websearch if I intend to use an unusual
extension in
a program on any OS. Just suppose you choose an extension that's
also
used by the "super dooper porn hunter" for your "work control

system" :)

Robert de Bath <robert\$ @ debath.co.uk> <<http://www.cix.co.uk/~mayday>>

[Also commented on by Steve VanDevender. PGN]

✶ Re: Pilot fixes faulty jet (Wienstock, [Risks 22.85](#))

<"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>>

Mon, 25 Aug 2003 09:48:32 +0200

This incident was reported on-line also by the BBC, citing The Times, at <http://news.bbc.co.uk/1/low/world/europe/3143237.stm>

Thanks to Harold Thimbleby for pointing it out to me.

It is important to get things right, and these news reports, from what are supposedly the best of British journalism, fail to do so.

The Times apparently suggested a bug in the computer providing a false indication:

The incident occurred on 8 Aug 2003 after a Boeing 757 run by British tour

operator MyTravel was found to have a faulty onboard computer that

insisted the aircraft was airborne when it was in fact parked on the

tarmac. Covered in oil after resetting a sensor in the aircraft's

nosewheel, the pilot [asked passengers.....] [[RISKS 22.85](#),

PGN-ing The

Times].

The BBC suggests a "faulty warning light":

The tourists had waited ... while the pilot fixed a faulty warning light

... The light had indicated the plane was airborne when it was still on the ground. After repairing it, the plane's captain [asked the passengers]

[A company spokesperson said] " He (the pilot) was confident that it was simply an indication error

In these brief reports there are three mutually incompatible hypotheses concerning the origin of the problem: a "faulty warning light", an ill-adjusted nosewheel sensor, and a "faulty onboard computer". The Times contradicts itself concerning the origin of the fault (citing two of the three above) and the BBC, supposedly reporting on The Times, contradicts both of The Times's hypotheses.

The BBC includes reader opinions on its news page. One may notice how ready people are to express opinions on the appropriateness of the captain's action, without having enough information to judge it. For the appropriateness of hiser gesture depends crucially on what was said, cf. the following two examples (for speech 2, I choose one of the three hypothesised causes and make some assumptions. This should not be taken to mean that I judge that this was the most likely interpretation of events. For I do not know).

1. "The airplane thinks it's in the air when it's on the ground. We think we've fixed what we guess the problem might be. We're going to risk it. Who wants to come with us?";

2. "We are getting a false air/ground indication. The consequences of that are that two of our three braking systems might not operate as intended on landing. The aircraft will stop safely on the runway with just wheel brakes; indeed the manufacturer had to prove that it would do so, and provide us with the performance figures, before we could fly anyone in the airplane. So the worst case outcome would be that we take a little longer to stop when we arrive at the destination.

I have tried to find the source of the problem. I checked the nosewheel sensor, which determines whether the nosewheel is in full contact with the ground. It was clearly out of adjustment, and that alone would have caused the problem we have been seeing. I have adjusted the sensor so that it now operates correctly. After checking everything else that we can, I assume that that is the only problem. Theoretically there could be a second problem, but I think that is unlikely enough that I shall ignore it, while remaining alert to potential signs of it when we fly. I am content to fly this airplane. Remember that my health and safety is on the line every bit as much as yours and I have family too. I recommend you be content to fly in this airplane also. But I wish to give those of you who think differently from us a choice."

Peter B. Ladkin, University of Bielefeld, Germany
<http://www.rvs.uni-bielefeld.de>

✦ **Satellite photo of Eastern North America during blackout**

<"John Oram" <risks@oram.com>>

Thu, 21 Aug 2003 17:37:37 -0700 (PDT)

The NOAA posted a few satellite photos of Northeastern North America before and after last week's blackout.

<http://www.noaanews.noaa.gov/stories/s2015.htm>

<http://www.noaanews.noaa.gov/nightlights/blackout081403-20hrsbefore-text.jpg>

<http://www.noaanews.noaa.gov/nightlights/blackout081503-7hrsafter-text.jpg>

The first photo seems a little supersaturated to me (and a little misaligned, making for a poor flip-back-and-forth...) but clearly show great swaths of New York, Ontario, Ohio and Michigan in the dark.

However, there is a surprising amount of light still on, especially in New York and Long Island, in line with the NYT article quoted by Andrew Greene in 22.87. Other major urban areas (Toronto, Detroit, Cleveland) seem much darker in comparison. Maybe more cars and generators in NYC and thus more ambient light?

[Clearly, some places were either better prepared or lucky (or both) than others. PGN]

✦ **2004 IEEE Symposium on Security and Privacy, Call for Papers**

<David Wagner <daw@cs.berkeley.edu>>

Sun, 24 Aug 2003 17:26:28 -0700 (PDT)

2004 IEEE Symposium on Security and Privacy

9-12 May 2004, The Claremont Resort, Oakland, California, USA

sponsored by

IEEE Computer Society Technical Committee on Security and Privacy

in cooperation with

The International Association for Cryptologic Research (IACR)

Paper submissions due: 5 Nov 2003

For submission guidelines see

<http://www.cs.berkeley.edu/~daw/oakland04-cfp.html>

For questions, please contact the program chairs:

oakland-pcchairs04@zurich.ibm.com

Symposium Committee:

General Chair: Lee Badger (DARPA)

Vice Chair: Steve Tate (University of North Texas)

Program Co-Chairs:

David A. Wagner (University of California, Berkeley, USA)

Michael Waidner (IBM Zurich Research Lab, Switzerland)



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

[ACM](#) Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 89

Tuesday 2 September 2003

Contents

- [Chips that can self-destruct](#)
[Kenneth Ng](#)
- [Diebold voting machines](#)
[John Paulson](#)
- [A new approach to roller coasters](#)
[Henry Baker](#)
- [Battling the threat of data extinction](#)
[NewsScan](#)
- [Man steals tracking device, which tracks him down](#)
[PGN](#)
- [Careful typography in the CAIB report](#)
[Craig DeForest](#)
- [EchoStar sued for `No-Call List' breach](#)
[Monty Solomon](#)
- [Bahrain's proposed smart ID cards](#)
[George Mannes](#)
- [802.11: When Is 54 Not Equal to 54?](#)
[Matthew Gast via Monty Solomon](#)
- [EarthLink sues to stop Alabama and Vancouver spammers](#)
[Monty Solomon](#)

- [Can't catch it? A virus can still hurt you.](#)
[Richard A. O'Keefe](#)
 - [Hackers cut off SCO Web site](#)
[Richard Forno via Dave Farber](#)
 - [More theories about Sobig vandal's motivation](#)
[NewsScan](#)
 - [Re: Sobig affects Amtrak trains, Air Canada](#)
[Scott Nicol](#)
 - [Re: "Good" worm fixes infected computers](#)
[Neil Youngman](#)
 - [More on the Davis-Besse worm attack](#)
[Martyn Thomas](#)
 - [Re: Satellite photo of Eastern North America during blackout](#)
[Dan Pritts](#)
 - [Re: Nasty elevator death at Houston hospital](#)
[Paul D. Walker](#)
[Richard H Miller](#)
 - [Re: Pilot fixes faulty jet](#)
[Daniel Lance Herrick](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ Chips that can self-destruct

<"Ng, Kenneth (US)" <kenng@kpmg.com>>
Mon, 25 Aug 2003 15:51:55 -0400

Michael Sailor and colleagues at the University of California at San Diego have developed a self-destruct mechanism that can be activated (with a warning) if a machine detects that it has been stolen. The first thought I had was "program bug". The second was "virus". The third was "cyber denial of service attack". Personally, it wouldn't be the same without the "this

chip will self destruct in 5 seconds, good luck, Jim" followed by the standard white smoke from Mission Impossible.

<http://www.newscientist.com/news/news.jsp?id=ns99991795>

[The technique involves adding gadolinium nitrate to silicon. PGN]

⚡ Diebold voting machines

<john paulson <munch@acm.org>>

Tue, 2 Sep 2003 11:57:59 -0700

The head of a company vying to sell voting machines in Ohio told Republicans in a recent fund-raising letter that he is "committed to helping Ohio deliver its electoral votes to the President next year."

<http://www.cleveland.com/election/index.ssf?/base/news/106207171078040.xml>

Inspired by remotely triggered self-destructing chips, how about voting machines that can be remotely instructed to add and subtract votes?

Well, you might say, why bother? It can already be done locally! PGN]

⚡ A new approach to roller coasters

<Henry Baker <hbaker1@pipeline.com>>

Thu, 28 Aug 2003 10:03:58 -0700

[FYI -- Note the use of Windows OS to run this thing. HB]
[Could give new meaning to the Blue Screen of Death. PGN]

``Roller coasters are boring. ... But a new two-seat ride called RoboCoaster is different. Its 4,400-pound, 22-foot-long mechanical arm provides a much wider array of twists and turns than any single traditional coaster can, its makers say. And because those whipping motions are just about infinitely programmable, riders can have radically different experiences on the same RoboCoaster, and can even customize their own thrills. ... Made by the German robotics company Kuka Roboter, the \$350,000 RoboCoaster became available last November. Fourteen have been installed, two of them in the United States - at American World Resort in Wisconsin Dells, Wis., and at C.J. Barrymore's, 30 miles north of Detroit. Ten are housed in a vast hall at the Legoland theme park in Billund, Denmark, where they are called Power Builders.

Riders use a Windows-based touch-screen computer to program their own RoboCoaster experience. There are seven levels of difficulty, and within each level are 14 movements -- dips, falls, rocket starts, butterfly rolls and loops - lasting 5 to 15 seconds. According to Legoland, more than 1.4 million combinations are possible. With six axes, the robot can throw riders in any number of directions, turning them upside down, spinning them side to side, or making them swoop as if they were in a jet fighter -- all at 1.9 G's, nearly twice the normal gravitational pull. Optical sensors attached to a motor in each axis calculate the position of the coaster's arm every 32 milliseconds. [Source: Taking Roller Coaster Limits

for a Ride,
Noah Shachtman, *The New York Times*, 28 Aug 2003; PGN-abridged]
<http://www.nytimes.com/2003/08/28/technology/circuits/28roll.html>
[?pagewanted=print&position=](#)

✶ Battling the threat of data extinction (NewsScan)

<"NewsScan" <newsscan@newsscan.com>>
Fri, 29 Aug 2003 09:35:18 -0700

Because most digital files are dependent on the operating systems in which they're stored and the software applications used to create and access them, would-be archivists are faced with the task of retaining and maintaining the digital hardware necessary to read digital files as well as the files themselves. "With each passing day, the reservoir of digital documents grows," says Eastman Kodak manager Andrew Lawrence. "Often, there is no associated hard-copy output to archive via conventional means. Over time, the problem is that media decays and hardware and software platforms evolve, placing the electronically stored information at risk." Lawrence suggests the best approach to digital preservation is a dual track. For short-term needs, users can maintain structured electronic archives in their native formats. But for longer-term purposes, Lawrence suggests creating a referenced archive of permanent document images in analog format, such as microfilm, that could provide a technology-proof repository.

Glenn Widener, director of Internet technology at Swiftview, has a different solution. He recommends using the Printer Control Language (PCL) format, invented by Hewlett-Packard for its LaserJet family of printers, as an easy way to preserve documents. "Many PCL viewers can view 15 to 20 years back. There will always be commercial tools readily available to read it." Meanwhile, Dan Schonfeld, director of products for Artesia, says his company's digital asset management software enables users to archive viewers, readers and players along with files. "Because we can store any type of media, we can actually store applications as well as the media files themselves."

[TechNewsWorld 28 Aug 2003; NewsScan Daily, 29 Aug 2003
<http://www.ecommercetimes.com/perl/story/31436.html>

🔥 Man steals tracking device, which tracks him down

<"Peter G. Neumann" <neumann@csl.sri.com>>
Mon, 1 Sep 2003 08:56:43 -0700 (PDT)

A man stole a \$2500 GPS-based computerized home-detention tracking device that had been temporarily left outside the home of the woman who was supposed to be wearing it. By the time she reported the loss, prison officials had already rounded up the thief. [Source: AP item 1 Sep 2003; PGN-ed]

<http://www.newsday.com/news/nationworld/wire/sns-ap-tracking-device,0,4015374.story?coll=sns-ap-nationworld->

[headlines](#)

[ADDED NOTE: The stolen device was apparently the transponder box.

I presume the anklet was not removable. PGN]

Careful typography in the CAIB report

<zowie@euterpe.boulder.swri.edu (Craig DeForest)>

Wed, 27 Aug 2003 15:19:13 -0600

I'm sure that many are reading and will contribute about the recent Columbia

Accident Investigation report:

<http://www.caib.us>

A rare amusing moment occurs on p. 191, where noted communication expert

Edward Tufte analyses the horrific viewgraph layout used within NASA.

One of Tufte's points is that even a simple unit measurement ("cubic inches") is laid out three different ways in a single viewgraph, making it difficult to recognize that the three units are directly comparable (in this case an analytical model that was designed for foam chunks up to 3 cubic inches was used for a foam chunk that was over 300 times larger). But a diligent copy editor has regularized the three layouts in the corresponding figure caption, obscuring Tufte's argument.

Tufte analysed the Challenger explosion in his fabulous book, "Visual Explanations". He convincingly argued that poor communication (caused in

part by bad charting of the relevant risk factors) played a significant role in the loss of Challenger. The same arguments seem to hold about Columbia.

✶ EchoStar Sued for `No-Call List' breach

<Monty Solomon <monty@roscom.com>>

Thu, 28 Aug 2003 08:54:27 -0400

The state of Missouri sued EchoStar Communications Corp. on 27 Aug 2003, accusing the satellite television giant of violating the state's telemarketing "no-call" list, wrongly calling residents who had home telephone numbers registered with the state's no-call list, pitching its satellite equipment and television services. [Source: Jim Suhr, AP Online, 27 Aug 2003; PGN-ed]

<http://finance.lycos.com/home/news/story.asp?story=35468386>

✶ Bahrain's proposed smart ID cards

<George Mannes <George.Mannes@thestreet.com>>

Thu, 28 Aug 2003 11:36:12 -0400

Bahrain Takes Swipe Into The Future With New Smart ID Cards, 26 Aug 2003, AP,

<http://www.informationweek.com/story/showArticle.jhtml?articleID=13900098>

Bahraini officials envision a photo ID card with a 64-kilobyte microchip

holding the card holder's name, address, national identification number, digital fingerprints and driver's license, passport, medical, financial and educational data. Users will be able to pay bills, withdraw cash, transfer money check their bank balances and conduct Internet transactions with a swipe of the card, and use the same card to votes in municipal and parliamentary elections. "We truly believe that this is going to improve and change things dramatically," Sheik Ahmed bin Ateyatella Al Khalifa, undersecretary of the Central Informatic Organization, told reporters Tuesday.

Improve and change things dramatically for whom? The article -- which says Bahrainis already used bar-coded ID cards for elections last October -- doesn't say. I'm guessing I'm not the only RISKS reader who'd be a tad concerned about the RISKS of having all my personal, medical, financial, educational -- and perhaps political-leanings -- data all in one convenient, centrally informatic, location.

***802.11: When Is 54 Not Equal to 54?**

<Monty Solomon <monty@roscom.com>>

Mon, 1 Sep 2003 04:11:22 -0400

When Is 54 Not Equal to 54? A Look at 802.11a, b, and g Throughput
by Matthew Gast, author of *802.11 Wireless Networks: The

Definitive Guide*

08 Aug 2003 (updated: 14 Aug 2003)

Now that the 802.11g standard has been finalized, comparisons with the other standards in the 802.11 family are inevitable. One conclusion that is frequently drawn is that 802.11g offers similar speeds to 802.11a. After all, both products are advertised as having a data rate of 54 Mbps.

This article develops a simple model for the maximum TCP throughput of 802.11 networks so that a comparison can move beyond a simple comparison of nominal bit rates. According to the model, 802.11g is significantly faster than 802.11b. In a network consisting only of 802.11g clients, it is even slightly faster than 802.11a. However, "protection" mechanisms added to 802.11g to ensure backwards compatibility with legacy 802.11b clients can cut the throughput by 50 percent or more. ...

http://www.oreillynet.com/pub/a/wireless/2003/08/08/wireless_throughput.html

⚡ EarthLink sues to stop Alabama and Vancouver spammers

<Monty Solomon <monty@roscom.com>>

Thu, 28 Aug 2003 08:51:12 -0400

Internet provider EarthLink Inc. said it sued operators in Alabama and British Columbia for flooding its network with some 250 million unwanted commercial messages, in an attempt to break their e-mail "spam"

rings --

which reportedly hide behind a veil of bogus Web sites and e-mail accounts

bought with stolen credit-card numbers. EarthLink estimates costs around \$5

million in employee time and wasted bandwidth. [Source: Andy Sullivan,

Reuters, 27 Aug 2003; PGN-ed]

<http://finance.lycos.com/home/news/story.asp?story=35464940>

✶ Can't catch it? A virus can still hurt you.

<"Dr Richard A. O'Keefe" <ok@cs.otago.ac.nz>>

Wed, 27 Aug 2003 15:41:08 +1200

I thought I was safe. My mail machine is an Alpha running OSF/1. I use mailx, which not only doesn't do anything in particular with attachments, it wouldn't know an attachment if one bit it in the backside. I suppose it's theoretically possible to write a virus or worm for the Alpha, but there's not that much thrill in persecuting orphans; the bad guys much prefer going after idiot boxes. So I thought no virus could possibly pose a threat to *my* mail.

Wrong.

My mail comes through the University's Information Technology Services.

Quoting their recent "ITS Incident Report: E-Mail Services #2",

E-Mail from off-campus destinations were lost by the University e-mail

system from approximately 5:00 am until 4:45 pm on August 23.

People will

have received an e-mail from the sender that contained no subject line or content.

In fact I received a couple of hundred such messages. How could that be?

Continuing the quote:

Since Wednesday August 20 [to Monday August 25] the University has

received over 120,000 copies of the Sobig-F virus. ... The University

e-mail hubs scan all e-mail messages for viruses. Any e-mail that

contains a virus is quarantined and no further delivery attempts are made.

The quarantined e-mail messages are occasionally analysed in order to

trace the origins of viruses, with old e-mail messages purged as required.

So far so good. They try hard to stop viruses getting through, and they monitor the bad stuff so they can do a better job. BUT

With the advent of Sobig-F, the number of e-mail messages quarantined grew

dramatically. The file system on the mailhubs only permits 32,000 files

per directory. On Thursday last week one of the mailhubs hit this limit.

At this time it was thought that the large number of quarantined e-mail

messages was due to historical data not being purged. However, another

32,000 virus infected e-mail messages were intercepted by each of the

mailhubs over the next 36 hours which caused similar failures to the one

on Thursday.

As a result of these failures, incoming e-mail messages could

not be

written to disk for virus and spam scanning. When the system went to send

on the e-mail to its destination, only the sender data was retained.

OOPS. In hindsight, it was a bad idea to store quarantined messages and

good ones on the same file system, and it might not have been such a good

idea to store each quarantined message as a separate file.

However, I'm

pretty sure I wouldn't have thought of that without the benefit of

hindsight.

The e-mail messages that have had their content lost are not recoverable.

The only way for you to know the contents of those e-mail messages is to

ask for the sender to resend the message(s). You are urged to take care

to only request a resend from known senders. In the event that a request

for a resent message is made to a spammer, you are likely to receive

greater volumes of spam in the future.

The really sad thing here is that the guys in ITS *do* have a clue or two,

and were trying to do their job.

ITS has now stopped reaining block e-mail messages containing viruses.

Oh dear. Retaining messages was a *good* thing. The sheer volume of bad

stuff has stopped them doing it. Death of the net? Oh yes, it's entirely

forgivable that they didn't spend a lot of time thinking about the problem

on Thursday, because tech support people around the campus have been as busy

as one-armed paperhangers trying to clean up after Blaster and Sobig-F.

Yes, they **do** stop those things entering through the network.

Yes, they

do provide up-to-date anti-virus software. However, people will run

Windows on their laptops, take them home, and bring the infection back...

Instead of just deleting all virus messages, I think it would be better to retain a random sample of (say) 30,000 of them.

So I've learned something: I can lose a couple of hundred messages because of a virus my machine didn't catch and cannot catch, because of what the virus did to a mail hub that didn't and couldn't catch it either.

I've also learned that if I receive e-mail without content or subject line, I probably shouldn't delete it all, like I did. Sigh.

[The quoted text was quite sloppy. Vastly too many "(sic.)"s have been

removed, and various garbles fixed to make this message more readable.

My apologies if I missed a few! PGN]

🔥 Hackers cut off SCO Web site (via Dave Farber)

<Richard Forno <rforno@infowarrior.org>

Mon, 25 Aug 2003 17:42:09 -0400

As an IT security professional but also someone who thinks the SCO-World case is loonier than Franken-Fox, I'm not sure whether to smirk with satisfaction or offer to help find the perpetrator....

Hackers cut off SCO Web site

By Martin LaMonica, CNET News.com, 25 Aug 2003

This weekend, a denial-of-service attack took down the Web site of The SCO

Group, which is caught in an increasingly acrimonious row with the open-source community over the company's legal campaign against Linux.

SCO's Web site was largely out of commission until Monday morning, a

representative of the Lindon, Utah-based Unix and Linux seller said Monday.

Performance measurement statistics from Netcraft indicated that the site had been down since Friday night.

In a distributed denial-of-service (DDoS) attack, numerous computers

simultaneously send so much data across a network that the targeted system

slows to a crawl while trying to keep up with the traffic it's receiving.

The SCO representative could not say where this weekend's strike originated.

However, unofficial open-source spokesman Eric Raymond suggested in a

posting Sunday to open-source news Web site NewsForge that the attack was

launched by someone angry at comments from SCO executives criticizing the

open-source community's role in the legal battles over Linux.

[...]

http://news.com.com/2100-1002_3-5067743.html?tag=fd_top

Source: Dave Farber's IP distribution

<http://www.interesting-people.org/archives/interesting-people/>

More theories about Sobig vandal's motivation

<"NewsScan" <newsscan@newsscan.com>>

Tue, 26 Aug 2003 08:28:20 -0700

Is money the real motivation for the spread of the Sobig virus? Sobig is transmitted as an e-mail attachment and is the sixth variant of the malicious code by an unknown attacker. Mikko H. Hypponen, director of antivirus research at F-Secure corporation in Finland says: "I think the motivation is clear: it's money. Behind Sobig we have a group of hackers who have a budget and money." Computer security expert Russ Cooper suggests that the vandal is acting out comic book fantasies: "You can liken this guy to Lex Luthor and we're all Supermen. Luckily, we've been able to get the kryptonite from around our necks each time so far." One popular theory is that Sobig is the work of an e-mail spammer who is aggressively trying to build a clandestine infrastructure for blitzing the Internet with junk e-mail. Antivirus software researcher Joe Hartman of TrendMicro says, "If machines remain infected they could be used in any kind of attack. The question we ask ourselves is, What is he trying to achieve? We don't think it's planned for a specific threat, rather its more likely a money-making spam scheme." And Bruce Hughes of Trusecure points out: "There is some evidence that he's been tied in with spammers." Sobig spreads further only when a computer user selects the attached program that then secretly mails itself to e-mail addresses stored in the user's computer. The

Computer

Emergency Response Team at Carnegie Mellon University says, "Our current advice is: Don't open an attachment unless you are expecting one." [*The New York Times*, 26 Aug 2003; NewsScan Daily, 26 August 2003] <http://partners.nytimes.com/2003/08/26/technology/26VIRU.html>

⚡ Re: Sobig affects Amtrak trains, Air Canada (Leisner, [RISKS-22.88](#))

<Scott Nicol <snicol@apk.net>>

Wed, 27 Aug 2003 22:17:34 -0400

According to a technically sparse press release by CSX

<[http://www.csx.com/?fuseaction=company.](http://www.csx.com/?fuseaction=company.news_detail&i=45722&news_year=-1)

[news_detail&i=45722&news_year=-1](http://www.csx.com/?fuseaction=company.news_detail&i=45722&news_year=-1)> ,

it wasn't the signalling computers that were affected, but rather the

communication lines that the signals are sent on. One would have to

assume this means that the communication lines that are used for signalling are also used for other purposes, including sending e-mail.

What happens when somebody inside CSX sends an e-mail to "all", on the

subject of, say, next years health plan choices, with a 20MB powerpoint

presentation attached? Do the signals get blocked for a few minutes until

the e-mail is dispatched everywhere?

⚡ Re: "Good" worm fixes infected computers (Schindler, [RISKS-](#)

22.87)

<Neil Youngman <no.spam.for.n.youngman@ntlworld.com.die.spammers>>

Wed, 27 Aug 2003 18:51:16 +0100

> Even though the new worm is "good," it can cause plenty of
> trouble for computer users ...

I remember discussing the topic of "good viruses" and why there was no such thing -- way back in 1989; see

<http://www.ja.net/CERT/CERT-CC/virus-1/archives/1989/v2i117>

Now I know of one company whose network was taken off line for at least 24 hours by this "good virus". A truly destructive "good virus" may have taken a long time to arrive but I'm sorry to see that it finally got here.

➤ More on the Davis-Besse worm attack ([RISKS-22.88](#))

<"Martyn Thomas" <martyn@thomas-associates.co.uk>>

Sun, 31 Aug 2003 15:00:15 +0100

"When the Davis-Besse nuclear power plant in Ohio was hit by the Slammer worm [in Jan 2003], the reactor happened to be off-line. But the worm disabled a safety monitoring system for nearly five hours. 'We are still working through the information to find out what happened', says a spokesman for Akron-based FirstEnergy, which owns the plant." [Source: *New Scientist*, 30 Aug 2003, page 5]

⚡ Re: Satellite photo of Eastern North America during blackout ([R-22.88](#))

<Dan Pritts <danno@deathstar.org>>

Wed, 27 Aug 2003 17:15:06 -0400

Given the population density, I would be shocked if there were not more cars and generators per square mile in metro NYC than anywhere else on the continent. Detroit and Cleveland are certainly much less densely populated than metro NYC (I don't know about Toronto but it can't be any MORE dense).

I would also expect that the saturation of generators is likely very low in all of these areas compared to the saturation of cars. Most families have multiple cars - few families have generators. Obviously not all the cars were on, but traffic snarls in NYC might also suggest that the commuters all were still trying to get home 7 hours later.

⚡ Re: Nasty elevator death at Houston hospital ([RISKS-22.87](#))

<"Paul D. Walker" <pdwalker@quagmyre.com>>

Sat, 23 Aug 2003 22:30:19 +0800

> RISKS reported the earlier cases in Ottawa [...]

Actually, there were three deaths that summer from elevators. I

lived in
Ottawa during that summer and since then I have become extra
cautious about
crossing elevator doors.

✶ Re: Nasty elevator death at Houston hospital

<rick@bcm.tmc.edu (Richard H Miller)>

Fri, 22 Aug 2003 10:08:51 -0500 (CDT)

> ... We also previously reported the Houston elevator that
failed
> in the floods caused by Tropical Storm Allison and by default
went down to
> the BOTTOM, drowning its occupant ([RISKS-21.47](#)).

Actually this is becoming a bit of an urban legend. The elevator
did not
take the woman down to the basement. What happened was the
several people
walked down to the lower levels of the garage to attempt to move
their cars
higher. [I believe it was the woman and a security guard]. In
the basement
level, a wall separating the garage from the bayou was
penetrated and the
water came rushing into the garage. The woman was picked up by
the water
and happened to be flung into the open elevator. Some of the
details may be
fuzzy but it was not a case of an elevator opening into a flood

Richard H. Miller, MCSE, Information Security Manager,
Information Technology
Security and Compliance, Information Technology - Baylor College
of Medicine

✈️ **Re: Pilot fixes faulty jet (Ladkin, [RISKS-22.88](#))**

<daniel lance herrick <herrick@pbs.proquest.com>>

Tue, 2 Sep 2003 13:42:16 -0400 (EDT)

Peter Ladkin's followup in [RISKS-22.88](#) had the URL of a BBC story on the incident. That story had a whole lot of (generally uninformed) comments added at the end. There was one highly informative contribution:

I was one of the passengers on this flight (with my wife and 2 young children) and have been amazed by the inaccuracy of the reporting on this event. The vote was not to see if we should "risk it" but merely whether passengers wanted to go the lengths of boarding the plane again (3rd time) to try and fly home. The only "risk" was that the plane would only be able to taxi to the end of the runway and because of the fault not start the initialisation sequence. We would then have had to go straight back to the terminal and wait at least another 4 hours for the engineers to be flown from the UK.

All the news I have read today is about a "patched" plane "personally repaired" by the pilot and then us voting whether we thought it was safe to fly, which is just not the case but obviously makes for a better headline. It is funny that the bit of oil on the pilots shirt has now become him being "caked" and "covered" in oil! Nigel, England

What a letdown!



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 90

Monday 8 September 2003

Contents

- [Men steal computers in high-security facility in Australia](#)
[David Landgren](#)
[Craig S. Bell](#)
- [Handicapped's gas pedal on left side of car leads to 3 injuries](#)
[Kurt Thams](#)
- [Blackout of mobile phone service in greater Frankfurt](#)
[Juergen Fenn](#)
- [Nuclear powerplants may not have firewalls!!](#)
[Marty Leisner](#)
- [Computer failures led to NE US blackout](#)
[Jeremy Epstein](#)
- [Trade group tells DHS don't use MS](#)
[PGN](#)
- [Curtailing online education in the name of homeland security](#)
[Jaeger/Burnett via Monty Solomon](#)
- [Secrecy and the Patriot Act](#)
[Amy Goldstein](#)
- [Identity Theft Victimizes Millions, Costs Billions \(Jennifer 8. Lee via Monty Solomon](#)
[<monty@roscom.com>](#)
- [Victims of identity theft and account theft](#)

[NewsScan](#)

- [California gets new privacy law](#)

[NewsScan](#)

- [ICANN takes hits from lawmakers](#)

[NewsScan](#)

- [The benefits and risks of robot surgery](#)

[Juergen Fenn](#)

- [WhereWare](#)

[Eric W. Pfeiffer via Monty Solomon](#)

- [Covert virus channels?](#)

[Rob Slade](#)

- [The dangers of remote start on a car with manual transmission](#)

[Jason Lunz](#)

- [Testing by Chimp? I think it too risky](#)

[Bob Heuman](#)

- [Info on RISKS \(comp.risks\)](#)

⚡ **Men steal computers in high-security facility in Australia**

<David Landgren <david@landgren.net>>

Sat, 06 Sep 2003 12:41:42 +0200

Two men gained access to a high-security computer facility at Sydney Internal Airport, passing themselves off as contractors. They disconnected and walked off with two computers on a trolley. The Australian Federal Police and ASIO (Australian Security Intelligence Organisation) would like to know as a consequence to what extent their operations have been compromised.

Where once again it is shown that security is only as good as its weakest

link:

<http://www.smh.com.au/articles/2003/09/04/1062548967124.html>

⚡ Men steal computers in high-security facility in Australia

<"Craig S. Bell" <craig@runbox.com>>

Sat, 06 Sep 2003 19:00:57 GMT

This appears to have been an inside job. The stolen hardware may contain sensitive security / anti-terror information. I wonder whether they ran any sort of monitoring software that noticed whether the application was running. Even if they were monitoring, would anyone have been able to show up or alert the guards in two hours?

Considering the level of security at a corporate datacenter that I frequent, I can easily foresee how such a thing can happen -- if you look like you know where you're going, you are rarely challenged by the superannuated private security guards, who often seem less aware of their surroundings than the janitorial staff.

⚡ Handicapped's gas pedal on left side of car leads to 3 injuries

<Kurt Thams <thams@thams.com>>

Tue, 2 Sep 2003 15:48:28 -0700 (PDT)

Two elderly women and a young man were hospitalized Monday after an

85-year-old Stockton man driving on the Santa Cruz Municipal Wharf

apparently mistook a car's gas pedal for the brake and struck four people.

[...] The car did not belong to (the driver) and had a gas pedal for

handicapped drivers that extends to the left side of the car.

[<http://www.santacruzsentinel.com/archive/2003/September/02/local/stories/01local.htm>

or

<http://tinyurl.com/m0x6>]

The article does not say whether there is any warning posted on the car that

the vehicle's controls are not like other cars. Even so, one wonders if any

driver accustomed to standard controls could avoid reflexively hitting the

gas when he meant to hit the brake.

⚡ Blackout of mobile phone service in greater Frankfurt

<Juergen Fenn <juergen.fenn@GMX.DE>>

Sun, 07 Sep 2003 00:22:29 +0200

Mobile phone services of Deutsche Telekom's subsidiary company T-Mobile in

the greater Frankfurt area were interrupted from 10am on 9 September 2003

until late evening when phones could be used again. A spokesman for

T-Mobile said in a statement to "heise online" that the failure was probably

due to a power blackout, or to a problem with the software the company is

using. The blackout initially was said to end after two hours (report in

German): <http://www.heise.de/newsticker/data/jk-04.09.03-004/>

Other

telephone companies were not affected.

⚡ Nuclear powerplants may not have firewalls!!

<"Marty Leisner" <mleisner@eng.mc.xerox.com>>

Mon, 08 Sep 2003 10:25:12 -0400

[Source: *The New York Times*, 7 Sep 2003]

<http://www.nytimes.com/2003/09/07/technology/07WORM.html>

[...] But an incident in January at the Davis-Besse Nuclear Power Station,

run by the FirstEnergy Corporation outside Toledo, Ohio, showed that this

was not always the case. The nuclear plant has not been generating power

since early 2002, but a computer system there that was not supposed to be

linked to the Internet was invaded by a worm known as Slammer, causing the

system to shut down for five hours. The event was not made public until

Kevin Poulsen reported it on Aug. 20 on SecurityFocus .com, an information-security news site.

Richard Wilkins, a FirstEnergy spokesman, said the company realized after

the worm struck that it did not have a firewall isolating its corporate

computers from the computers controlling the reactors, but that it now had

such a safety precaution in place.

SIX months after the Davis-Besse problem, the North American Electric

Reliability Council, the industry group overseeing the

electrical grid,
announced that there were "documented cases in which bulk
electric system
control was impaired" by the same worm. It recommended that
utility
companies separate the computers running their power grids
from their
corporate networks.

I'm amazed by so many things...including they use commercial,
virus-plagued
operating systems systems to run their infrastructure.

⚡ Computer failures led to NE US blackout

<Jeremy Epstein <jeremy.epstein@webmethods.com>>

Thu, 4 Sep 2003 10:03:11 -0400

According to the WashPost, transcripts of telephone
conversations released
by the House Energy and Commerce Committee show that computer
failures in
monitoring the transmission lines left the operators blind.
That meant they
couldn't tell what was happening or control the systems, leading
to the
power surge that caused the blackout.

<http://www.washingtonpost.com/wp-dyn/articles/A22588-2003Sep3.html>

Readers of RISKS shouldn't be the least bit surprised...

⚡ Trade group tells DHS don't use MS

<"Peter G. Neumann" <neumann@csl.sri.com>>

Tue, 2 Sep 2003 15:36:49 -0700 (PDT)

The Computer & Communications Industry Association (CCIA) has urged the Department of Homeland Security to reconsider its decision to use Microsoft software on its desktop and server systems, citing "major security failures" created by the raft of vulnerabilities in MS's products.

<http://www.crn.com/sections/BreakingNews/dailyarchives.asp?ArticleID=44258>

✶ Curtailing online education in the name of homeland security

<Monty Solomon <monty@roscom.com>>

Wed, 3 Sep 2003 01:23:36 -0400

Curtailling online education in the name of homeland security:
The USA
PATRIOT Act, SEVIS, and international students in the United States
by Paul T. Jaeger and Gary Burnett

ABSTRACT

Online courses have become an important part of the academic offerings of many institutions of higher education in the United States. However, the homeland security laws and regulations enacted since September 2001, including the USA PATRIOT Act, have created serious limitations on the ability of international students studying in the United States to participate in online educational opportunities. Placing online education within the context of the mutually beneficial relationships

between international students and the United States, this article examines the assumptions and the impacts of these regulations on the students and the institutions of higher education. This article explores the enrollment limitations in online courses for international students in terms of information policy and concepts of presence and identity in online environments, offering an examination of the implications of this issue for education and information in United States.

CONTENTS

Introduction: The United States of America, immigrants, and visitors

International students in the United States

The USA PATRIOT Act and international students

Restrictions on the online education of international students

Identity and presence in online environments

Conclusion: The policy picture for education and information

http://firstmonday.org/issues/issue8_9/jaeger/index.html

✶ Secrecy and the Patriot Act (Amy Goldstein)

<"Peter G. Neumann" <neumann@csl.sri.com>>

Mon, 08 Sep 2003 09:59:02 -0400

[Source: Fierce Fight Over Secrecy, Scope of Law;
Amid Rights Debate, Law Cloaks Data on Its Impact
By Amy Goldstein, *The Washington Post*, 8 Sep 2003; Page A01;
PGN-excerpted from a long and informative article]

<http://www.washingtonpost.com/wp-dyn/articles/A40110-2003Sep7.html>

In Seattle, the public library printed 3,000 bookmarks to alert patrons that the FBI could, in the name of national security, seek permission from a secret federal court to inspect their reading and computer records -- and prohibit librarians from revealing that a search had taken place.

In suburban Boston, a state legislator was stunned to discover last spring that her bank had blocked a \$300 wire transfer because she is married to a naturalized U.S. citizen named Nasir Khan.

And in Hillsboro, Ore., Police Chief Ron Louie has ordered his officers to refuse to assist any federal terrorism investigations that his department believes violate state law or constitutional rights. [...]

By its very terms, the Patriot Act hides information about how its most contentious aspects are used, allowing investigations to be authorized and conducted under greater secrecy. As a result, critics ranging from the liberal American Civil Liberties Union to the conservative Eagle Forum complain that the law is violating people's rights but acknowledge that they cannot cite specific instances of abuse. [...]

This summer, two major lawsuits were filed challenging the Patriot Act's central provisions. The Republican-led House startled the administration in July by voting to halt funding for a part of the law that allows more delays in notifying people about searches of their records or belongings. And the GOP chairmen of the two congressional committees that oversee the Justice Department have warned Ashcroft that they will resist any

effort, for now,
to strengthen the law.

Identity Theft Victimizes Millions, Costs Billions

<Monty Solomon <monty@roscom.com>>

Thu, 4 Sep 2003 23:01:39 -0400

Source: Article by Jennifer 8. Lee, 4 Sep 2003

<http://www.nytimes.com/2003/09/04/politics/04IDEN.html>

About 3.3 million American consumers discovered within the last year that their personal information had been used to open fraudulent bank, credit card or utility accounts, or to commit other crimes, according to the Federal Trade Commission's first national survey on identity theft. The commission, in a report issued today, said these cases had collectively cost businesses \$32.9 billion and consumers \$3.8 billion.

In addition, 6.6 million people fell victim to account theft in the last year. Unlike identity theft, in which the criminal uses personal information to open and use accounts that are in the victim's name, account theft entails using stolen credit or A.T.M. cards, or financial records, to steal from the victim's existing accounts.

Such account-theft cases, the survey found, caused \$14 billion in business losses and \$1.1 billion in consumer losses. The vast majority of these cases, almost 80 percent, involved credit card fraud.

Though account theft and identity theft are often lumped together in popular perception, data from the survey showed that the consequences of identity theft were more severe. In identity theft, which accounted for nearly 10 million of the 27 million cases of both types in the last five years, the financial losses were greater, and it took victims longer to resolve the cases. [...]

✶ Victims of identity theft and account theft

<"NewsScan" <newsscan@newsscan.com>>

Thu, 04 Sep 2003 09:17:35 -0700

[...] Half of all victims knew the method by which the thieves had obtained the personal information. About 25% of the victims said the information had been stolen through either the mail or the loss of a wallet, and 13% percent said it had been stolen in the course of a purchase or another transaction.

[*The New York Times*, 4 Sep 2003; NewsScan Daily, 4 Sep 2003]
<http://partners.nytimes.com/2003/09/04/politics/04IDEN.html>

✶ California gets new privacy law

<"NewsScan" <newsscan@newsscan.com>>

Thu, 28 Aug 2003 08:30:19 -0700

California has just passed privacy legislation aimed at preventing banks, insurance companies and other institutions from sharing their personal information, and Gov. Gray Davis said: "Most Californians are stunned to learn that financial corporations trade their names for money. That is wrong, and when I sign this bill, that practice will stop." The law will require permission from a customer before financial institutions share any information on that customer with an unaffiliated company or an affiliated firm in a different line of business. [AP/*USA Today*, 28 Aug 2003; NewsScan Daily, 28 Aug 2003]
http://www.usatoday.com/tech/news/techpolicy/2003-08-28-davis-privacy-bill_xhtm

✶ ICANN takes hits from lawmakers

<"NewsScan" <newsscan@newsscan.com>>

Fri, 05 Sep 2003 08:30:32 -0700

Rep. Howard Berman (D-Calif.) is critical of ICANN (the Internet Corporation for Assigned Names and Numbers) for not doing enough to stop scammers and child pornographers from registering under false names with stolen credit cards: "I'm disappointed with the failure of the marketplace and regulators to deal with this problem. A legislative solution seems necessary." And Rep. Lamar Smith (R-Texas) agrees: "There's not a real seriousness of intent either by ICANN or the Department of Commerce to have

an accurate whois database." Commerce Department General Counsel Theodore

Kassinger says that ICANN is busy working on solving the problem. [Reuters/*USA Today*, 4 Sep 2003; NewsScan Daily, 5 September 2003]

http://www.usatoday.com/tech/news/techpolicy/2003-09-04-net-id-checks_x.htm

⚡ The benefits and risks of robot surgery

<Juergen Fenn <juergen.fenn@GMX.DE>>

Sun, 07 Sep 2003 00:11:40 +0200

The benefits and risks of robot surgery have been discussed in press reports in Germany recently. A medical robot constructed to make operations for inserting artificial hip and knee joint implants more precise has been criticised for allegedly causing severe harm to at least a small number of patients, German news magazine DER SPIEGEL reported recently (in German):

<http://www.spiegel.de/spiegel/vorab/0,1518,262585,00.html>

<http://www.spiegel.de/spiegel/0,1518,262637,00.html>

The reports are claiming "about two dozen cases" would be considered by medical experts as some former patients are seeking compensation for rather severe damages to their muscles and nerves after undergoing operations. Ten lawsuits are pending at a Frankfurt court. According to DER SPIEGEL a Los Angeles law firm is said to represent some American patients who underwent surgery at a clinic at Frankfurt, Germany, specialising in this

kind of
operations suing the American manufacturer of the system in mass
action at a
Californian court.

The report admits, however, that some 6000 operations have been
done in all.

Most operations are said to have been successful.

In a press release the body responsible for the clinic has said
the system
is also used in Korean and Japanese clinics routinely. Using
"Robodoc" meant
putting considerably less strain on patients than traditional
methods. It is
said to be working rather reliable. The risks of post-surgical
complications
would be much smaller than without the system which has already
been used
for 10 years (in German):

<http://www.hvbg.de/d/pages/presse/preme/robodoc.htm>

A presentation of the robot's capabilities can be found at

<http://www.robodoc.com/eng/robodoc.html>

WhereWare

<Monty Solomon <monty@roscom.com>>

Mon, 25 Aug 2003 11:00:59 -0400

By Eric W. Pfeiffer, Sep 2003, *Technology Review*

<http://www.technologyreview.com/articles/pfeiffer0903.asp>

Soon, hardware and software that track your location will be
providing directions, offering shopping discounts, and aiding
rescue

workers-services that promise a windfall for ailing telecom carriers.

Amanda sits idly at the bar of the trendiest restaurant in town, twirling a swizzle stick and sipping a cocktail. But cool as she looks, she's feeling anxious: her date is nearly 15 minutes late. She considers calling him but doesn't want to seem nervous or overeager. Still, she pulls out her cell phone, only instead of calling, she opens a special menu, enters his number, and sees that he is at the corner of Prospect and Broadway, not more than three minutes away. When he walks in, Amanda brushes off his apology, saying she wasn't at all worried.

Sound fanciful-or outright implausible? Lock on to location-based computing, the hottest thing in wireless, which offers new services to customers and new revenue streams to carriers, and could save lives in the process. The idea is to make cell phones, personal digital assistants, and even fashion accessories capable of tracking their owners' every movement-whether they're outdoors, working on the 60th floor, or shopping in a basement arcade. Already, Japanese telecommunications company KDDI offers over 100 different location-based services using technology developed by wireless-equipment maker Qualcomm, from bracelets to let parents track their kids in the park, to cell phones that point the way to cheap noodle shops in Tokyo's skyscraping Shinjyuku district. In Korea, two million citizens use their cell phones to locate nearby friends and, for example, find the most

convenient coffee shops for impromptu meetings. In Europe, cell-phone networks can locate users and give them personalized directions to Big Ben, or the Eiffel Tower. [...]

✂ Covert virus channels?

<Rob Slade <rslade@sprint.ca>>

Wed, 3 Sep 2003 15:56:59 -0800

I am under attack. Or, at least, it feels like it.

Craig, in Atlanta, has a broadband connection, from atlantabroadband.com.

He also has Sobig. And he's been sending me between 60 and 100 infected messages *per hour* for the past couple of days. (He seems to turn his machine off at night. Thank goodness.)

That's about all I can find out about Craig, given his email headers:

```
Received: from CRAIG (81.cpe.atlantabroadband.com [64.30.ZZZ.ZZ]
(may be
forged)) by vcn.bc.ca (8.11.7+Sun/8.11.7) with ESMTTP id
h83LZkX08894 for
<rslade@vcn.bc.ca>; Wed, 3 Sep 2003 14:35:47 -0700 (PDT)
```

After all, Sobig isn't one of those viruses, like Sircam and Klez, that steals info from your machine and broadcasts it all over the net.

Or is it?

Given the number of messages I've received from him over the past two days, I've got a pretty complete list of the email addresses on his

machine.

Not knowing the rag, I don't know whether I'm supposed to be impressed that he is in contact with Intelligencer@NewYorkMag.com. He seems to be into self-promotion--premierlistny@aol.com and ratings@about-inc.com. And maybe trying to set up his own business (ezcreationsltd@yahoo.com)? He *does* seem to be trying to better himself, maybe get an education (ZZZZZZ@learnlink.emory.edu and LearnLinkinfo@learnlink.emory.edu). He might be aware that something is wrong with his machine: he seems to be rather eclectic in terms of where he goes for help (hot-line@microsoft.hr, InfoService@microsoft.at, mssupport@gbrands.com, mswgulf@microsoft.com).

All of this may be due to an impending marriage: is he searching for an engagement ring (info@shimmerandstone.com)? And, if so, does his fiancée know about help@nudesonline.com, sal@freeZZZ.ws, salform@freeZZZ.ws, sassyemail@yahoo.com, and support@bigbonerbonus.com?

[x changed to Z above in hopes of getting by a few filters.
PGN]

Then again, maybe he's a terrorist: mts@lebanon-online.com.lb.

(For those both ethical and unobservant, I have tried to mung anything that seemed to identify any person.)

rslade@vcn.bc.ca slade@victoria.tc.ca rslade@sun.soci.niu.edu
<http://victoria.tc.ca/techrev~rslade> or <http://sun.soci.niu.edu/~rslade>

⚡ The dangers of remote start on a car with manual transmission

<Jason Lunz <lunz@falooley.org>>

Wed, 3 Sep 2003 14:23:13 -0400

[This story appeared on a local chat mailing list. It's forwarded to

RISKS and rewritten for brevity with permission. Jason]

An online acquaintance of mine has a manual-transmission car with remote start option. On Saturday, a stuck antenna switch on the console needed to be cleaned. The car was parked, out of gear, with the hand brake on. To operate the switch, the hand brake had to be released, so the car was put in gear to stop it from rolling. The antenna switch was cleaned and returned to working order.

On Sunday when the car was next needed, its state was momentarily forgotten. The remote start button was pressed several times. Nothing happened. The car alarm was disarmed, and trunk opened for loading. The remote start button was tried again, this time with disastrous results. The car started, then proceeded driverless over a curb, over some rosebushes, over a sapling, and over an embankment wall.

The risk is obvious. Why would it be possible for a remote start feature to engage with the car in gear? My automatic-transmission car won't shift out of park unless a safety interlock is disengaged, and the safety won't operate unless I put my foot on the brake. It's not clear why something as potentially dangerous as a remote start system

wouldn't
take similar precautions.

🔥 Testing by Chimp? I think it too risky

<rsh@idirect.com>

Tue, 02 Sep 2003 21:57:17 -0400

How do I describe the risks of using programs tested by Chimps paid 45 cents per hour (Banana Dollars?)... This is definitely outsourcing, but who is it who is out of their mind?

Found at http://www.itworldcanada.com/index.cfm/ci_id/47258.htm

Chimps go ape for Visual Basic 6.0

Funny enough, this is no joke [*]. A company in Des Moines, Iowa is teaching computer programming skills to chimpanzees and has plans to resell their services in outsourcing contracts. Primate Programming Inc. recently conducted research that claims computer programming is a task that most higher primates can perform. And, according to the company, the primate programming language of choice is Microsoft Corp.'s Visual Basic 6.0. Primate Programming is offering software maintenance and report writing services -- all conducted by chimpanzees -- for approximately US \$0.69 per hour. The company also offers software testing for US\$0.45 per hour -- a lower price since the chimps require less skill to conduct tests. Visit

www.newtechusa.com/ppi/main.asp for more information.

[* It is much too early -- or too late -- for April Fools' Day, and this one

has been around for quite a while, but I sort of regret having ignored it

previously, so why not now? The Web site has matured a little since.

PGN]



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 91

Thurs 18 September 2003

Contents

- [VeriSign's Site Finder profits from typos](#)
[NewsScan](#)
- [VeriSign change to .com/.net behavior](#)
[Matt Larson via Monty Solomon](#)
- [VeriSign DNS change broke my HP printer](#)
[John Leyden via Lindsay Marshall](#)
- [London blackout caused by incorrect relay fitting](#)
[Phil Thornley](#)
- [Lockheed Martin accident with satellite](#)
[Gerrit Muller](#)
[Craig S. Bell](#)
- [E-Voting Audit Ready for Public](#)
[Kim Zetter via Monty Solomon](#)
- [Instant message: you're under arrest](#)
[NewsScan](#)
- [Yahoo requests ATM card pin nos.!!](#)
[Chris J. Brady](#)
- [Utterly amazing spam/scam?](#)
[Drew Dean](#)
- [How to Steal \\$65 Billion: Why Identity Theft is a Growth Industry](#)

[Robert X. Cringely via Dave Farber](#)

● [Dave Barry column results in denials of service to telemarketers](#)

[Max](#)

● [Cehck tihs out!](#)

[Jim Schindler](#)

● [Call for papers: IWIA 2004](#)

[Stephen D.B. Wolthusen](#)

● [REVIEW: "Desktop Witness", Michael A. Caloyannides](#)

[Rob Slade](#)

● [Info on RISKS \(comp.risks\)](#)

⚡ VeriSign's Site Finder profits from typos

<"NewsScan" <newsscan@newsscan.com>>

Tue, 16 Sep 2003 09:22:06 -0700

Internet registrar VeriSign has launched a new service, Site Finder, that offers users who mistype a URL a list of alternative Web sites that they might be trying to reach. Several ISPs do the same thing -- most notably AOL and MSN -- but critics say that because VeriSign controls the directory computers for ".com" and ".net" names, they could easily reroute all queries to Site Finder. "We put so much of our research into developing this AOL search result page," says an AOL spokesman. "We are reviewing our potential options. We are strongly opposed to them interjecting themselves into our members' search experience." Site Finder's suggestions include both standard search results and pay-for-placement advertisements, which are identified as such. But while VeriSign VP Ben Turner says the new service is designed to

"improve overall usability of the Internet," Danny Sullivan, editor of Search Engine Watch, warns that Site Finder's capabilities could also be abused -- by directing users only to pay-for-placement sites, for instance. Meanwhile, the new service provides a much-needed new revenue stream for the Internet registrar. "Right now, VeriSign's business is not a growing business, and anything that they do to add the slightest amount of growth is going to be positive," says an analyst with U.S. Bancorp Piper Jaffray. [AP 15 Sep 2003; NewsScan Daily, 16 September 2003] <http://apnews.excite.com/article/20030915/D7TJ2U500.html>

[This move by VS has caused huge reactions within the Internet community.

We include just a few items here from among what is available on the Net,

as a sample. The list of reasons why this is a very foolish move by VS is

enormous. Apparently, the folks who really should have known that this

was going to happen did not, and were blindsided. DNS disablers are being

developed to circumvent the VS strategy, but the net results are ugly.

See the People For Internet Responsibility (PFIR) statement by Lauren

Weinstein, PGN, and Dave Farber:

<http://www.pfir.org/statements/vs-domain-abuse>

PGN]

VeriSign change to .com/.net behavior

<Matt Larson (via Monty Solomon)>

Mon Sep 15 19:32:04 2003

[<http://www.merit.edu/mail.archives/nanog/msg13603.html>]

Today VeriSign is adding a wildcard A record to the .com and .net zones.

The wildcard record in the .net zone was activated from 10:45AM EDT to

13:30PM EDT. The wildcard record in the .com zone is being added now. We

have prepared a white paper describing VeriSign's wildcard implementation, which is available here:

<http://www.verisign.com/resources/gd/sitefinder/implementation.pdf>

By way of background, over the course of last year, VeriSign has been

engaged in various aspects of Web navigation work and study.

These

activities were prompted by analysis of the IAB's recommendations regarding

IDN navigation and discussions within the Council of European National

Top-Level Domain Registries (CENTR) prompted by DNS wildcard testing in the

.biz and .us top-level domains. Understanding that some registries have

already implemented wildcards and that others may in the future, we believe

that it would be helpful to have a set of guidelines for registries and

would like to make them publicly available for that purpose.

Accordingly,

we drafted a white paper describing guidelines for the use of DNS wildcards

in top-level domain zones. This document, which may be of interest to the

NANOG community, is available here:

<http://www.verisign.com/resources/gd/sitefinder/bestpractices.pdf>

Matt Larson <mlarson@verisign.com>

VeriSign Naming and Directory Services

⚡ VeriSign DNS change broke my HP printer (John Leyden)

<"Lindsay Marshall" <Lindsay.Marshall@newcastle.ac.uk>>

Wed, 17 Sep 2003 12:48:37 +0100

<http://www.theregister.co.uk/content/6/32872.html>

VeriSign DNS change broke my HP printer, By John Leyden, *The Register*,
17 Sep 2003

LettersReg readers have plenty of say about VeriSign's controversial move to direct surfers who get lost on the Web to a search site run by the company.

Our coverage provoked a large number of letters, almost all hostile, about VeriSign's audacious typo-squatting land grab:

"All your Web typos belong to us"

Martin Ward is the first to fire brickbats at the company, which Reg readers have rechristened as "VeriSlime".

VeriSign are essentially "squatting" on every unregistered domain name, and using them for profit. How many trademarked names does that include? What are the fines for squatting on just *one* trademark for commercial exploitation?

Roger Thomas worries about the implications if other DNS providers adopt VeriSign's tactics.

That's a worrying article, and just thinking about the issues raised I can see the following:

1) If it's good enough for VeriSign to mess about with the root servers I

can see other DNS providers doing the same, by redirecting users to their own systems.

2) This will poison DNS servers across the world as they will end up caching

the SOA records created by VeriSign for these 'dynamic' DNS entries.

While the time to live on these records is short, real entries will be

dropped as the junk entries are added to the database. There is now a new

DNS attack where nodes on the Internet create vast numbers of random DNS

look up requests so clearing the DNS caches of all the DNS servers they access.

[...]

⚡ London blackout caused by incorrect relay fitting

<Phil Thornley <phil.thornley@baesystems.com>>

Thu, 11 Sep 2003 11:00:28 +0000

Britain's biggest blackout for 25 years, which plunged large parts of London into darkness, was the result of a one-amp fuse being fitted in place of a five-amp fuse at a substation.

The Guardian, 11 Sep 2003:

<http://www.guardian.co.uk/transport/Story/0,2763,1039722,00.html>

The full report is available at:

<http://image.guardian.co.uk/sys-files/Guardian/documents/2003/09/10/London28082003.pdf>

[An offer they could not refuse! PGN]

✶ Lockheed Martin accident with satellite

<Gerrit Muller <gerrit.muller@embeddedsystems.nl>>

Thu, 11 Sep 2003 08:35:56 +0200

Goddard Space Flight Center: Earth Science Missions Anomaly Report:

GOES/POES Program/POES Project: 6 Sep 2003

<http://www.spaceref.com/news/viewsr.html?pid=10299>

As the NOAA-N Prime spacecraft was being repositioned from vertical to horizontal on the "turn over cart" at approximately 7:15 PDT on 6 Sep 2003, it slipped off the fixture, causing severe damage. The 18' long spacecraft was about 3' off the ground when it fell. The mishap was caused because 24 bolts were missing from a fixture in the "turn over cart". Two errors occurred. First, technicians from another satellite program that uses the same type of "turn over cart" removed the 24 bolts from the NOAA cart on September 4 without proper documentation. Second, the NOAA team working today failed to follow the procedure to verify the configuration of the NOAA "turn over cart" since they had used it a few days earlier.

IMPACT ON PROGRAM/PROJECT AND SCHEDULE: The shock and vibration of the fall undoubtedly caused tremendous damage. Significant rework and retest will be required. NOAA-N Prime is planned for launch in 2008.

CORRECTIVE ACTION: Lockheed Martin formed an Accident Review Team in which GSFC is participating. The immediate actions concern safety (preventing the spacecraft from rolling, discharging the batteries, and depressurizing the propulsion system). NOAA-N Prime is under guard, all records have been impounded, and the personnel interviewed. After the safety issues are addressed, attention will focus on assessing the damage to NOAA-N Prime.

✶ Lockheed Martin accident with satellite

<"Craig S. Bell" <craig@runbox.com>>

Wed, 17 Sep 2003 02:40:22 GMT

So, Lockheed Martin dropped my satellite! [I say "my" because I reckon that my U.S. tax dollars are paying for NOAA equipment.]

Under-construction satellite drops to floor in mishap:

<http://www.sfgate.com/cgi-bin/article.cgi>

[?file=/news/archive/2003/09/09/state1637EDT0153.DTL](http://www.sfgate.com/cgi-bin/article.cgi?file=/news/archive/2003/09/09/state1637EDT0153.DTL)

Risks: Never move anything worth \$239M (regardless of it's technological complexity, or overall robustness) without first making sure that you can do so without utterly dropping it! I imagine that it would be

relatively easy
to check for the presence or absence of a few load-bearing bolts
beforehand.

Also, because the poor thing was energized, they can't even go
examine it to
see how bad the damage is. It may be a number of days before we
truly know
the effects of dribbling satellites. Somebody is going to get a
bad
performance review this year.

There is a purportedly exclusive photograph on Efed Company
(most of you
know the site I mean). I would include the link; but, I know
that this
would merely be filter-bait. =-) The photo can be easily found
on the front
page.

Just how many companies are there building satellites these
days? Could a
relative lack of competition have anything to do with it; or, is
the market
healthy? This can't be good for business (even if the customer
just awarded
you some extra rocket launches that were surrendered by your
misbehaving
competitor).

⚡ E-Voting Audit Ready for Public

<"monty solomon" <monty@roscom.com>>

Thu, 18 Sep 2003 11:54:08 -0400

By Kim Zetter, Wired.com, 18 Sep 2003

A security audit ordered by Maryland Gov. Robert Ehrlich on
Diebold

Election Systems' touch-screen voting machines is complete, and a version of it is ready for public consumption.

Shareese DeLeaver of the governor's office said the 200-page report has been shown to Diebold officials and is now being reviewed by the state's Department of Budget and Management and the State Board of Elections. The report was commissioned by the governor after researchers at Johns Hopkins University and Rice University discovered serious security flaws (PDF) in code for the AccuVote-TS voting terminals.

A redacted version of the report, with information useful to malicious crackers taken out, will be available on the state's Web site Friday or early next week. The severity of Hurricane Isabel and the amount of energy the governor's office must devote to recovery from the storm will determine the timing of the report's posting.

Last month Gov. Ehrlich charged Science Applications International, or SAIC, in San Diego with conducting the audit before the state would proceed with a \$55.6 million purchase and servicing contract for Diebold's electronic voting machines. Ehrlich said it was imperative the government ensure the integrity of the election process by conducting "a thorough, fully independent review of the Diebold system."

Diebold has maintained that its system has no security vulnerabilities. ...

<http://www.wired.com/news/technology/0,1282,60486,00.html>

✶ Instant message: you're under arrest

<"NewsScan" <newsscan@newsscan.com>>

Thu, 18 Sep 2003 09:00:30 -0700

The investigation of a Wall Street trading scandal (in which a former Bank of America broker has been charged with grand larceny and securities fraud) is the first case that has used a chain of evidence derived from the instant messaging records of licensed brokers and dealers. Instant messaging (IM) systems are now widely used on Wall Street and to a large extent have replaced traditional e-mail. One attorney who consults on electronic communications said a New York Stock Exchange executive's question about instant messaging was: "Wait a minute, is that what my 13-year-old daughter uses at home?" The answer: "I said yes -- and your traders." [**USA Today**, 18 Sep 2003; NewsScan Daily, 18 Sep 2003]
http://www.usatoday.com/tech/techinvestor/techcorporatenews/2003-09-18-ims_x.htm

✶ Yahoo requests ATM card pin nos.!!

<chris.j.brady@britishairways.com>

Wed, 17 Sep 2003 13:06:41 +0100

There's a scam e-mail going round purporting to come from Yahoo. It is a bulk e-mail stating that anyone with a Premium Account (that is

one where you
pay by credit card for extra e-mail storage) needs to update
their account
details or else the account will be closed. The e-mail links to
the following
page: <http://yahoo-wallet.com/> When you click on the link you
get a form
requesting your:

Yahoo E-mail address,
Password,
First Name,
Last Name,
ZIP code,
Debit or Credit Card no.,.
Expiration Date AND -
Debit / ATM Pin. no. <==== NOTE THIS !!

The form has the Yahoo logo and appears innocuous, but why
do they
want passwords and pin nos.?

The risks are obvious - but this e-mail is either the most
stupidest yet and
if it comes from Yahoo then they have learned nothing about such
scams in
the years that they have they been in the Internet business. And
if it is a
scam then it is the most blatant fraud on the Internet yet. Of
course e-mail
to abuse@yahoo.com remain ignored.

Utterly amazing spam/scam?

<Drew Dean <ddean@csl.sri.com>>
Thu, 11 Sep 2003 17:03:37 -0700 (PDT)

I've recently received 2 spams from the same people. In one

message,
they offer: (1) heroin, (2) "Tomohawk" [sic] rockets, (3)
cocaine,
(4) (sex) slaves, (5) counterfeit currency, and (6) child
pornography,
among other commodities. Their "special offers" are rather
beyond belief,
too.

The mail itself appears to have been sent from Japan, based on
Received:
headers added by SRI's mailservers. (Or they're perfect
forgeries, which is
extremely unlikely for reasons I won't go into here.) The URL
in the
message goes to a Web site for which the whois database gives
contact info
in Thailand, but the server itself physically appears to be in
Florida (at
least according to traceroute). (Why I am not surprised that
these people
are downstream from Global Crossing?) Tracking down contact e-
mail info
takes a detour via Latin America, but would seem to eventually
end up in
Missouri, although with Arizona contact information. There's a
US toll-free
number to call the spam-list manager, and a mailing address in
Florida.

Now, I can't imagine anyone actually responding to this: (1) it
could
be a sting operation, although that's kind of hard to imagine.
"Your
Honor, I didn't really expect a missile, but I wanted to see what
they'd send me instead...." (2) As you'd be committing a felony,
you
can't go to law enforcement if the deal goes wrong, hence the
prevalence of violent crime among criminals. However, this
requires
that you be able to find the other party....

It's also worth noting that the price of illegal narcotics

depends

greatly on where you are in the world: smugglers demand risk pay. It's not at all clear where these people are offering delivery.

Meta-RISK: How many e-mail filters will this message trip?

Drew Dean, Computer Science Laboratory, SRI International

✶ How to Steal \$65 Billion: Why Identity Theft is a Growth Industry

<Dave Farber <dave@farber.net>>

Sat, 13 Sep 2003 08:51:35 -0400

[excerpt from an article by Robert X. Cringely, PGN]

Recently my mail was stolen. It wasn't supposed to be stolen, which is a given, but it also wasn't supposed to be able to be stolen because I was out of town for two weeks and had the Post Office hold my mail. Only it turns out that in Santa Rosa, California at least, holding mail means different things to different mail carriers. Someone -- a substitute carrier I'm told -- saw that big old pile of mail down at the post office (the pile with the big "vacation hold" sign above it) and thought what the heck I'll just deliver that mail anyway. And so they did. That big old pile of mail sat in my big old mail box on my little old country road under a walnut tree and across from a pond and sometime in the next few days it was stolen. The only reason I know any of this is because a neighbor eventually found some of my mail and some of a lot of other people's mail strewn along

the road like errant unmarked bills after a bank heist.

Here is something you probably didn't know. If you have the Post Office

hold your mail and they do something stupid like NOT hold it for some

reason, as happened to me, you have no recourse. [...]

<<http://www.pbs.org/cringely/pulpit/./index.html>>

✶ Dave Barry column results in denials of service to telemarketers

<Max <max7531@earthlink.net>>

Thu, 11 Sep 2003 12:51:03 -0700

Dave Barry column gives telemarketers headaches, 11 Sep 2003

<http://www.thekcrachannel.com/news/2474750/detail.html>

Now it's the telemarketers who are refusing to answer their phones, thanks

to a weekend column by *Miami Herald* columnist Dave Barry. The American

Teleservices Association was targeted by Barry in his 31 Aug 2003 column.

Barry urged readers to call the ATA and "tell them what you think" about

telemarketers. Thousands have done so, forcing the association to stop

answering its phones. Callers now hear a recording, which says that because

of "overwhelming positive response to recent media events, we are unable to

take your call at this time." ATA director Tim Searcy said the added calls

will be costly to his group because of toll charges and staffing issues.

Barry's only response is to sarcastically say he feels "just terrible,

especially if they were eating or anything."

[American Teleservices Association: (877) 779-3974]

⚡ Cehck tihs out!

<Jim Schindler <Jimschin@pacbell.net>>

Wed, 17 Sep 2003 10:44:28 -0700

Cehck tihs out.

Aoccdrnig to a rscheearch at Cmabrigde Uinervtisy, it deosn't mttar in waht oredr the ltteers in a wrod are, the olny iprmoetnt tihng is taht the frist and lsat ltteer be at the rghit pclae. The rset can be a total mse and you can sitll raed it wouthit porbelm. Tihs is bcuseae the huamn mnid deos not raed ervey lteter by istlef, but the wrod as a wlohe. Amzanig huh?

[This has been circulating around the Net. I'm not sure wehre it orginitaed. Apogolies to nonEgnilsh sepakres. PGN]

⚡ Call for papers: IWIA 2004

<wolt@igd.fhg.de (Stephen D.B. Wolthusen)>

Tue, 16 Sep 2003 19:57:03 +0200

Call for Papers, Second IEEE International Information Assurance Workshop
8-9 April 2004 -- University of North Carolina at Charlotte, NC, USA

Sponsored by the IEEE Computer Society Task Force on
Information Assurance

in cooperation with the
ACM Special Interest Group on Security, Audit, and
Control

Full paper submissions due: October 10th, 2003

Full CfP as well as PostScript and PDF versions of the call:

<http://www.iwia.org/2004/>

Accepted papers will be published by IEEE Press in a proceedings
volume.

Program Chair, Stephen D. Wolthusen, Fraunhofer-IGD,
Fraunhoferstr. 5,

64283 Darmstadt GERMANY Tel +49 (0) 6151 155 539 | Fax: +49 (0)
6151 155 499

REVIEW: "Desktop Witness", Michael A. Caloyannides

<Rob Slade <rslade@sprint.ca>>

Tue, 9 Sep 2003 12:27:44 -0800

BKDSKWTN.RVW 20030819

"Desktop Witness", Michael A. Caloyannides, 2002, 0-471-48657-4

%A Michael A. Caloyannides

%C 5353 Dundas Street West, 4th Floor, Etobicoke, ON M9B 6H8

%D 2002

%G 0-471-48657-4

%I John Wiley & Sons, Inc.

%O 416-236-4433 fax: 416-236-4448

%P 366 p.

%T "Desktop Witness: The Do's and Don'ts of Personal Computer
Security"

The title and the subtitle of this book are somewhat at odds.

Is this text

about the evidence that can be extracted from desktop machines?

Or is it

about protecting yourself and your personal computer or information?

Caloyannides would seem to be making the point that the answer is both: that there is an overwhelming need to ensure that your computer isn't finking on you, and that you must make every effort to ensure that the government cannot obtain the information on your desktop. While he is clearly on the personal side of the privacy versus national security debate, even those who agree with him may find the arguments shrill and extreme.

The subtitle of chapter one; indicating that the material is the author's opinion; should warn the reader that the discussion is editorial rather than closely reasoned. Caloyannides may, however, have hurt his own case by taking an anarchistic and almost paranoid position in stating the need for privacy against government encroachment. He does make a number of valid points, but misses other grounds that might have been convincing to a much wider audience, such as the point that the responsibility of protecting your own information is recognized in such legal areas as the difference between patent and trade secret. (A patent offers control over a device for a limited time as long as the technology is disclosed, whereas a trade secret offers protection for unlimited time as long as reasonable efforts are made to protect the information from disclosure.) The major point of chapter two appears to be that the use of encryption could, in and of itself, land you in trouble, and you should prepare to either hide the fact that encryption is taking place, or have a diversionary explanation ready for the

authorities. (The recommended use of one-time-pad technology and variant keys is technically interesting, but is unlikely to survive beyond a first use. Ironically, it seems to support a point that the author made earlier: "clever" tricks that rely on obscurity provide very poor protection.) The types of information that might be available from your computer, or Internet connection, are discussed in chapter three. The material ranges over a number of topics and has a difficult structure: some points are raised more than once and there are a number of related issues that are not mentioned at all. Means of recovering some of the data, and of getting rid of it, are reported, but not consistently.

Chapter four lists a vast array of protective measures. Most are very useful. Depending upon your situation, many will be considered overkill. Some are questionable: Caloyannides makes a blanket recommendation to install all operating system patches, but notes that doing so for some versions of Windows requires you to give away a lot of information. He does not, though, detail the times that official patches have made the situation worse rather than better, nor the complexity of some patches: by mid-2002 one expert noted that an effective installation of the Windows NT operating system required twenty nine steps, including no less than three separate installations of the latest service pack at different points. Oddly, while this section is supposed to review measures for computers not connected to networks, some of the points relate to activities on the

Internet.

Protection for connected machines is discussed in chapter five, with a heavy emphasis on the usage of the PGP encryption system. There is also an interesting insistence that steganography *is* an effective means of hiding communications: while Caloyannides points out a number of pitfalls in the use of the technology he does not mention detection measures, such as the ease of determining excessive entropy in the low-order bits of graphic images used to hide files. Secure telephony is discussed in chapter six.

The legal issues reviewed in chapter seven are mostly related to recent legislation providing for additional search authority. The author does include material and actions from outside the United States. The editorial finish in chapter eight warns against a society where everything must be homogenized in order to be safe.

In many places the book suffers from very poor copy editing. There are a great many instances of improper punctuation, sentence fragments, and words or phrases dropped into apparently unrelated text. Generally speaking one can discern the meaning, but deciphering the organization and intention of a section can be difficult. (Given the thrust of the book, is the author embedding hidden messages?)

While there are issues of general security in the book, it is, first and last, about privacy, and primarily personal privacy. The material could have been structured more usefully, and written less stridently, but a great

deal of helpful content is included. Those interested in privacy will find it interesting, and computer forensic specialists may also find it to be a handy reference.

copyright Robert M. Slade, 2002 BKDSKWTN.RVW 20030819
rslade@vcn.bc.ca slade@victoria.tc.ca rslade@sun.soci.niu.edu
<http://victoria.tc.ca/techrev/~rslade> or <http://sun.soci.niu.edu/>



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

[ACM](#) Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 92

Monday 6 October 2003

Contents

- [Near-disaster on a French commuter train](#)
[Alexandre Kampouris](#)
- [Nuclear reactor guard asleep on the job](#)
[Ken Knowlton](#)
- [Houston 911 System prone to crashes](#)
[Mark H. Johnson](#)
- [Continental Airlines takes back free miles](#)
[Frank](#)
- [Overlooked security risk: the telephone](#)
[NewsScan](#)
- [Parking chaos in York](#)
[David Wj Stringer-Calvert](#)
- [Torvalds: geeky kids need dates](#)
[NewsScan](#)
- [Computer blamed for bad pictures shown to Mexico's first lady](#)
[Mark Lutton](#)
- [Spam Abounds](#)
[Peter G. Neumann](#)
- [Fighting spam: raise the bridge or lower the water?](#)
[NewsScan](#)

- [VeriSign agrees to suspend Site Finder service](#)
[NewsScan](#)
 - [Purveyor of unencrypted service insists it's secure](#)
[Alice Silverberg](#)
 - [Another case of electronic vote-tampering?](#)
[Farhad Manjoo via Monty Solomon](#)
 - [AntiVirus autoresponders](#)
[Rob Slade](#)
 - [REVIEW: "Intrusion Signatures and Analysis", Stephen Northcutt et al.](#)
[Rob Slade](#)
 - [Rebuttal of review of my book by Rob Slade](#)
[Michael Caloyannides](#)
 - [Info on RISKS \(comp.risks\)](#)
-

⚡ **Near-disaster on a French commuter train**

<Alexandre Kampouris <ak@Radio-BIP.qc.ca>>

Mon, 22 Sep 2003 18:10:46 +0200

On Saturday September 20th, a disaster was miraculously averted when a RER suburban train stopped around 7:30 PM between stations near Villeneuve-Triage south of Paris due to equipment failure. According to the preliminary reports, the engineer, who is the only staff member on board, is said to have instructed the passengers over the PA system to alight the train on the left side, and walk to the next station. However it appears that the doors where only open on the right side; the passengers simply started walking on the second track. For a reason yet to be determined the traffic hadn't been interrupted in the other direction, and an oncoming train narrowly missed the myriads of passengers in its path, who

by sheer

luck escaped death or serious injury by throwing themselves to the ground or jumping aside.

An enquiry is underway. Even though the exact chain of events is yet to be established, there seems to be at least two system failures, i. e., (1) the doors opening on the wrong side, and (2) the non-secured track. The frightening event was recorded on video.

<http://infos.francetv.fr/semiStatic/64-NIL-NIL-259414.html>

<http://www.leparisien.com/home/info/faitsdivers/article.htm?articleid=210899112>

✶ Nuclear reactor guard asleep on the job

<KCKnowlton@aol.com>

Sun, 28 Sep 2003 14:37:07 EDT

[Quoted from *The New York Times*, Metro Section, 28 Sep 2003, pg 43, by Matthew L. Wald]

When two Nuclear Regulatory Commission officials found a security guard asleep at his post at the Indian Point 2 nuclear reactor last year, the agency decided not to issue a notice of violation because there was no terrorist attack on the plant during the half-hour or so that the guard was sleeping, a Congressional audit has found. ... The report also says the commission did not treat the incident more seriously because no guards

had been found sleeping "more than twice during the past year."

There was no comment in the story (or in the NRC report?) about sleeping behavior of those who deal with knobs, dials, monitors and keyboards.

An interesting general philosophical attitude: post-hoc shrugs for all infractions that had no catastrophic consequences.

🔥 Houston 911 System prone to crashes

<Mark_H_Johnson@raytheon.com>

Fri, 3 Oct 2003 08:39:55 -0500

To summarize - Houston has deployed a new 911 emergency response system which has had a number of failures since it went "live" a week ago.

Pictures of the new facility look somewhat like Mission Control - large consoles with multiple displays in front of each operator. It sure looks nice, but the system does not appear to work reliably.

The latest incident occurred during the day when technicians were working on the link between the computers and units within the cars. To quote:

When the system started slowing, technicians reverted to the backup, which

crashed within minutes. From 9:50 a.m. to 10:30 a.m., dispatchers resorted

to dispatching by radio instead of by computer. Without the computer's

locator system, they frequently had to ask emergency workers to volunteer

for individual assignments rather than assigning them to calls.

Another notable quote is

But city officials say the only way to test the system was by going "live."

Sorry, but that does not sound reasonable to me.

For reference:

<http://www.chron.com/cs/CDA/ssistory.mpl/metropolitan/2133809>

<http://www.chron.com/cs/CDA/ssistory.mpl/metropolitan/2134381>

<http://www.chron.com/cs/CDA/ssistory.mpl/metropolitan/2127855>

<http://www.click2houston.com/editorials/2522205/detail.html>

[May not all be permanent...]

✈ Continental Airlines takes back free miles

<frank099@earthlink.net>

Thu, 18 Sep 2003 22:28:45 -0500 (GMT-05:00)

Last week, I checked my Continental Airlines OnePass frequent flyer account and discovered that my account had been credited with 500,000 bonus miles, allegedly because I won a contest. It turns out that thousands of other people were "winners" as well, with some having a million or more frequent flyer miles added to their accounts. The miles didn't last long and were removed a few days later. However, many people had booked trips with those free miles, which Continental quickly canceled.

<http://www.usatoday.com/travel/news/2003/09/15-airmiles.htm>

Overlooked security risk: the telephone

<"NewsScan" <newsscan@newsscan.com>>

Thu, 02 Oct 2003 09:28:34 -0700

As corporate phone systems become increasingly complex and computerized, criminals are finding new ways to infiltrate company networks, and the problem becomes magnified as businesses turn to IP-based phone systems.

"This is the first time that a computer virus can stop your telephones from working," says PricewaterhouseCoopers senior manager Mark Lobel.

"There is a whole new class of attacks that can occur. The essence of the problem is that everyone is looking at this as a new technology for voice -- the way we're sending voice communications is absolutely new. But the data is still riding on the same infrastructure that was pounded by recent problems like SoBig." To counteract the threats, phone system administrators need to be much more vigilant about password management and may even consider locking out certain country codes. "In fact, you should probably consider the risk associated with VoIP systems to be as high as the threats to your organization's most sensitive data. If someone in your IT department gets paged when your firewall goes down, they should also be paged when 40 new voicemail boxes mysteriously appear on your IP system," says Lobel.

[*E-Commerce Times*, 2 Oct 2003; NewsScan Daily, 2 Oct 2003]

<http://www.ecommercetimes.com/perl/story/31731.html>

⚡ Parking chaos in York

<"David Wj Stringer-Calvert" <david.stringer-calvert@sri.com>>

Mon, 06 Oct 2003 11:41:08 -0700

The system controlling York's newly installed intelligent traffic variable-message signs (VMS) were hit by a computer virus on 4 Oct 2003, freezing 21 VMS displays at car parks that were intended to show the number of available parking space. Motorists thus went into full car parks expecting to find space. One VMS at St George's Field showed 349 spaces when there were **none**, causing an enormous traffic tie-up. [And no one was around to slay St George's draggin' congestion.] A similar problem had occurred in August. (The system, costing 1.5 million pounds, began operation in July 2003. The software is provided by Tennet and the hardware by Variable Message. A temporary fix is sought to enable the VMSs to be blanked out if this happens again. [Source: 'Frozen' signs lead to car park chaos, by Rosslyn Snow, **Yorkshire Evening Press**, 6 Oct 2003; PGN-ed]

⚡ Torvalds: geeky kids need dates

<"NewsScan" <newsscan@newsscan.com>>

Mon, 29 Sep 2003 14:17:45 -0700

Asked how to end virus and worm attacks, Linux creator Linus Torvalds told an interviewer: "When you have people who hook up these machines

that weren't designed for the Internet, and they don't even want to know about all the intricacies of network security, what can you expect? We get what we have now: a system that can be brought down by a teenager with too much time on his hands. Should we blame the teenager? Sure, we can point the finger at him and say, 'Bad boy!' and slap him for it. Will that actually fix anything? No. The next geeky kid frustrated about not getting a date on Saturday night will come along and do the same thing without really understanding the consequences. So either we should make it a law that all geeks have dates -- I'd have supported such a law when I was a teenager -- or the blame is really on the companies who sell and install the systems that are quite that fragile." [*The New York Times Magazine*, 28 Sep 2003; NewsScan Daily, 29 Sep 2003]

<http://partners.nytimes.com/2003/09/28/magazine/WLN104109.html>

✶ Computer blamed for bad pictures shown to Mexico's first lady

<"Mark Lutton" <Mark.Lutton@dialog.com>>

Wed, 1 Oct 2003 10:18:00 -0400

The wife of Mexican President Vicente Fox is a staunch defender of family values. Attending a charity presentation dedicated to helping children with cancer, she viewed a picture of a naked man and woman together that was somehow inadvertently included among the slides. A "technical

error" is
blamed.

[Source: Mexico's prim first lady gets eyeful of nudes, Reuters,
1 Oct 2003]

[http://www.reuters.co.uk/newsArticle.jhtml?
type=oddlyEnoughNews&storyID=3536434](http://www.reuters.co.uk/newsArticle.jhtml?type=oddlyEnoughNews&storyID=3536434)

[Let's see if this issue gets spam-filtered. PGN]

Spam Abounds

<"Peter G. Neumann" <neumann@csl.sri.com>>

Fri, 3 Oct 2003 10:34:42 PDT

Unfiltered spam has once again taken a quantum leap. The latest version of SpamAssassin catches about 1000 spams per day on e-mail to Neumann and RISKS. However, even after SpamAssassin does its job, RISKS is still getting about 90% spam from the residual mail. In other words, I have to delete almost all of the incoming mail to RISKS. My own mail is only somewhat less offensive. (And I have been away, which makes it ever more difficult to keep up. I regret the long gap between issues, and my inability to cope with the backlog in the past weeks. PLEASE resubmit any really salient items that you felt I might have missed. I need a salient solution to help overcoming being as-salted.)

Spam is evermore not your friend.

[Minor change in archive copy removing ambiguity. PGN]

✈ Fighting spam: raise the bridge or lower the water?

<"NewsScan" <newsscan@newsscan.com>>

Mon, 06 Oct 2003 09:46:36 -0700

Many software experts now believe that the best way to fight spam is not by targeting it directly but instead by concentrating on the identification of legitimate mail. VeriSign executive Nico Popp explains, "People have been spending all their time creating filters to find the bad guys. We want to turn that on its head and find ways to identify the good guys and let them in." The idea would be to develop the Internet equivalent of caller ID, with a technology that identifies senders and lets receivers presume that unidentified senders are sending junk mail. Richard Reichgut of AuthentiDate says, "It's not easy to change something as successful and widely used as e-mail. But the only way to fix e-mail is to have a strong way to know who is sending you mail." [**The New York Times**, 6 Oct 2003;

NewsScan Daily, 6 Oct 2003]

<http://partners.nytimes.com/2003/10/06/technology/06SPAM.html>

[Once again, see Lauren Weinstein's Tripoli proposal --

<http://www.pfir.org/tripoli-overview>

-- which is a sensible approach to giving users control over how to confront the e-mail dilemma. BEWARE of ceding this authority to ISPs!

PGN]

[Also, see "Four Internet pioneers discuss the sorry state of online

communication today. The consensus: It's a real mess." by Katharine Mieszkowski, Salon.com:

http://www.salon.com/tech/feature/2003/10/02/e_mail/

She quotes Dave Farber, Dave Crocker, Brad Templeton, and Jakob Nielsen.

PGN]

VeriSign agrees to suspend Site Finder service

<"NewsScan" <newsscan@newsscan.com>>

Mon, 06 Oct 2003 09:46:36 -0700

VeriSign and ICANN reached a temporary truce Friday, with VeriSign acquiescing to ICANN's demand that it suspend its controversial Site Finder service pending further technical review. ICANN could have fined VeriSign as much as \$100,000 or even revoked its contract to manage the master list of .com and .net Internet domain names. Critics have charged VeriSign with undermining the collectivist culture of the Internet with the preemptive launch of its service, which redirects Web users who mistype a URL to the VeriSign Web site. "In the past when you made a dramatic change to the network structure that was the least bit potentially damaging, you went out through the community and you exposed what you were going to do and got reaction," says Carnegie Mellon computer science professor David Farber. VeriSign "just broke the whole process." In its defense, VeriSign

executives say they notified ICANN of their plans ahead of time, but admitted that they sidestepped ICANN's lengthy approval process because it's too slow. In response, ICANN says it's "sympathetic to concerns" about its process and has proposed a more streamlined procedure for reviewing new services such as Site Finder. [*Wall Street Journal*, 6 Oct 2003; NewsScan Daily, 6 Oct 2003]

<http://online.wsj.com/article/0,,SB106519977252395300,00.html>

(sub req'd)

[This is after VeriSign told ICANN to drop dead: See the correspondence

<http://www.icann.org/correspondence/lewis-to-twomey-21sep03.htm>

and Dan Gillmor's column in response:

<http://weblog.siliconvalley.com/column/dangillmor/archives/001361.shtml>

noted courtesy of Dave Farber's IP. PGN]

🔥 Purveyor of unencrypted service insists it's secure

<Alice Silverberg <alice.silverberg@cs.stanford.edu>>

Fri, 3 Oct 2003 15:21:02 -0700

Here's a hotel reservation url that expects you to send your credit-card information unencrypted (though when you phone the associated number to ask about it, they insist that it's secure):

<http://www.innsuites.com/>

Another case of electronic vote-tampering? (Farhad Manjoo)

<Monty Solomon <monty@roscom.com>>

Sun, 5 Oct 2003 13:20:43 -0400

Another case of electronic vote-tampering?
Representatives of the computer vote-counting industry are
unfairly
dominating the standard-setting process, say critics.

By Farhad Manjoo, Salon.com, 29 Sep 2003

When the IEEE, the world's leading professional society of
engineers,
decided in the summer of 2001 to create a technical standard for
electronic
voting machines, most everyone concerned with the elections
business thought
it was a grand idea.

For the most part, the IEEE operates just as you'd expect a
bunch of
engineers to behave -- the group is rigorous, open-minded,
dispassionate,
and reluctant to embark upon any major endeavor unless everyone
with an
opinion has had an opportunity to hold forth. "Consensus" is
the IEEE's
main buzzword; and while that ethic can lead to some
frustration, it also
explains why so many industries and government agencies ask the
IEEE to draw
up technical standards for new technologies. People trust the
IEEE's open
process, and when it sets down certain specifications --
governing
everything from aircraft gyros to wireless networks -- the specs
are widely
respected by technologists.

And by the summer of 2001, a standard for voting machines was
clearly

needed. After the hobbled 2000 presidential election, officials across the nation were rushing to purchase new equipment to replace their maligned punch-card systems. Elections vendors were heavily promoting fully electronic, ATM-style touch-screen voting machines, but many computer scientists warned -- and are warning still -- of critical security flaws in such systems. The key players in the debate over electronic voting saw the IEEE as a good place to resolve concerns people had with the new systems; they hoped that after hearing all sides, the vaunted body could create respected technical guidelines for the machinery of modern democracy.

Two years later, however, the IEEE group charged with drafting a voting machine standard is paralyzed by bitter in-fighting. Members of the body can't agree on the substance of a proposed standard for voting machines, nor can they even come to a consensus on a fair process for determining such a standard.

The parties involved are arguing about big things -- about whether, for instance, electronic voting machines should be required to produce a "voter-verifiable" audit trail, which many security experts say is the only way to guarantee security in electronic systems -- and tiny things, such as the order in which topics are discussed in the meetings they hold. To hear members of the committee tell it, the whole process has become a circus -- a circus that illustrates how difficult it might be to eventually create a

national standard for voting systems. [...]
[http://www.salon.com/tech/feature/2003/09/29/
voting_machine_standards/](http://www.salon.com/tech/feature/2003/09/29/voting_machine_standards/)

✶ AntiVirus autoresponders

<Rob Slade <rslade@sprint.ca>>
Sun, 5 Oct 2003 13:35:27 -0800

I notice the NTBUGTRAQ seems to have added to following as a sigblock to all messages:

"Most viruses these days use spoofed e-mail addresses. As such, using an AntiVirus product which automatically notifies the perceived sender of a message it believes is infected may well cause more harm than good. Someone who did not actually send you a virus may receive the notification and scramble their support staff to find an infection which never existed in the first place. Suggest such notifications be disabled by whomever is responsible for your AV, or at least that the idea is considered."

Note once again that variations may occur. The infected user may be identified in Swen infected messages by the Return-Path header. Frequently the infected user's mailbox has been filled and is over quota, so the postmaster, abuse, and possibly support accounts should be notified as well. (The abuse and support I accounts that I have contacted who have taken the

time to investigate have confirmed that users identified in the Return=Path headers are infected.)

rslade@vcn.bc.ca slade@victoria.tc.ca rslade@sun.soci.niu.edu
<http://victoria.tc.ca/techrev/~rslade> or <http://sun.soci.niu.edu/~rslade>

REVIEW: "Intrusion Signatures and Analysis", Stephen Northcutt et al.

<Rob Slade <rslade@sprint.ca>>
Wed, 1 Oct 2003 07:54:59 -0800

BKINSIAN.RVW 20030831

"Intrusion Signatures and Analysis", Stephen Northcutt et al, 2001,
0-7357-1063-5, U\$39.99/C\$59.95/UK#30.99
%A Stephen Northcutt stephen@sans.org
%A Mark Cooper
%A Matt Fearnow
%A Karen Frederick
%C 201 W. 103rd Street, Indianapolis, IN 46290
%D 2001
%G 0-7357-1063-5
%I Macmillan Computer Publishing (MCP)
%O U\$39.99/C\$59.95/UK#30.99 800-858-7674 info@mcp.com
%O <http://www.amazon.com/exec/obidos/ASIN/0735710635/robsladesinterne>
 <http://www.amazon.co.uk/exec/obidos/ASIN/0735710635/robsladesinte-21>
%O <http://www.amazon.ca/exec/obidos/ASIN/0735710635/robsladesin03-20>
%P 408 p.
%T "Intrusion Signatures and Analysis"

Intrusion detection and network forensics are now vitally important topics in the security arena. An explanation of how to identify dangerous signatures, and extract evidence of an intrusion or attack from network logs, is something that most network administrators require. Unfortunately, while the idea is good, and badly needed, the execution, in the case of the current work, is seriously flawed.

The introduction doesn't really specify a purpose or audience for this book. Mention is made of the GIAC (Global Incident Analysis Center, also seemingly referred to at times as the GCIA) certification, but no definition is given as to what this actually is. Chapter one presents a number of examples of network log entries and formats. The interpretation, though, concentrates on easily identifiable items such as IP addresses, and neglects components that are less well known. There seems to be some attempt to structure the descriptions, but it is unclear and confusing, as are a number of the illustrations and figures.

Chapters three and four list a "top ten" of specific attacks, described down to a byte level, but not always in clear detail. Perimeter logs, such as those from firewalls and routers, are discussed in chapter six. Restraint in reaction to odd traffic is urged in chapter seven, particularly in light of the probability of address spoofing. Chapter eight outlines packets that indicate mapping scans, while nine does the same with searches that might be gathering system information. Denial of services attacks are reviewed in chapters ten and eleven, first with respect to attacks that

attempt

to exhaust specific resources, and then in regard to bandwidth consumption. Chapter twelve discusses trojan programs, concentrating on detection of unusual open ports. Miscellaneous exploits are listed in chapter thirteen, but since exploits are listed throughout the previous three chapters it is difficult to find a distinctive for this section. Fragmentation attacks are described in chapter fifteen. Chapter sixteen reports on some odd looking non-malicious packets, in warning against reacting to false positives. A grab bag of odd packets is listed in chapter seventeen.

As should be evident from the description above, there is a good deal of valuable material in this book. Unfortunately, it is not easy to extract the useful bits. The book as a whole could use serious reorganization. While chapter one appears to be an introduction to the technical details, a far better explanation of packets and the import of various fields is given in chapter five, ostensibly on non-malicious or normal traffic, and this material should probably have been placed at the beginning of the manual. Chapter fourteen, almost at the end of the text, reviews buffer overflows, which are seen throughout the chapters preceding it. There is a slight attempt to explain the book in chapter two, but the content and organization is perplexing, there is heavy use of unilluminated insider jargon, and the presentation of example packets and subsequent conclusions without the middle step of identifying the items that make these data suspicious could be quite frustrating to the student. The new system administrator will not find the explanations clear or

illuminating.

The experienced professional will not find particular attacks or traffic types easy to find for reference. Both groups will find themselves flipping back and forth between sections of the book, or even between sections of the exegesis of one particular attack.

However, both groups will likely be interested in the book anyway, simply because of the lack of other sources.

copyright Robert M. Slade, 2003 BKINSIAN.RVW 20030831
rslade@vcn.bc.ca slade@victoria.tc.ca rslade@sun.soci.niu.edu
<http://victoria.tc.ca/techrev/~rslade> or <http://sun.soci.niu.edu/~rslade>

⚡ Rebuttal of review of my book by Rob Slade ([RISKS-22.90](#))

<Michael Caloyannides <Michael.Caloyannides@mitretek.org>>
Wed, 01 Oct 2003 16:00:23 -0400

In his 9 Sep 2003 review of the book "Desktop Witness", 0-471-48657-4, Rob Slade made numerous factually incorrect statements that your readers are likely to be misled by.

A careful reading of the book would have shown that reviewer that steganography using conventional software is explicitly discouraged (rather than encouraged as he incorrectly claims) in the book precisely because it is detectable through steganalysis tools that look for statistical irregularities in the composite file; a careful reading of that same section would have shown the reviewer -- and anyone else -- that the

book then

proceeds to show that unconventional steganography is inherently undetectable because there is a multiple infinity of ways to embed a hidden meaning in an overt act, especially if it used rarely and if the ratio of covert to overt message is low. Who can credibly detect a steganographic content in a recipe for lasagna posted in some Usenet newsgroup, or in the presence of an occasional spelling error or in a graphic included in an otherwise professional document?

As with the steganography example, so with the rest of the points he raises;

his objections are based on a superficial reading of the book he reviewed that missed the points discussed in that book. For example, he sets the biased tone of his review by postulating an inconsistency in the title and subtitle of the book ("Desktop Witness". The Dos and Don'ts of Personal Computer Security), when it is quite clear that there is no such inconsistency because the book provides "the dos and dont's of personal computer security" so that one's desktop computer will not end up being used as a witness against one.

Worse yet, his review is repeatedly tainted with his religious objection to the fundamental premise of the book which is that honorable civilized people have a right to their privacy. While Mr. Slade's religious background, which includes a degree in Christian Science, is his own business, it is allowed to distort what should have been a factual review with his own value judgments. One reads, for example, in his review his assertion that the

book's reasoned arguments in support of individual privacy are "shrill", "extreme" or "paranoid". These oddly emotional words in a supposedly detached review are at best suspect, given the fact that: a) According to the FBI, roughly 1 in 20 Americans has been the victim of identity theft, and the trend is increasing at an alarming rate. b) There is a huge and healthy debate today about the extent to which individual privacy and the Bill of Rights should be sacrificed in the post 9/11 world.

For a balanced review of the same book by a University professor in the UK, your readers may also wish to read

<http://www.newscientist.com/opinion/opbooks.jsp?id=ns23486>

This book, by the way, is used in a number of Universities for training students in computer science as well as in law.



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

[ACM](#) Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 93

Tuesday 7 October 2003

Contents

- [Walter Cronkite: The New Inquisition](#)
[Chuck Messall via Dave Farber](#)
- [Re: Spam abounds](#)
[PGN](#)
- [California spammin'](#)
[NewsScan](#)
- [Worm FAQ](#)
[Stuart Staniford](#)
- [Jury convicts man in DMCA case](#)
[Paul Festa via Monty Solomon](#)
- [Broward considers dumping \\$17 million in touch voting machines](#)
[Kim Alexander](#)
- [Diebold voting machines in Volusia County FL](#)
[Brent M.P. Beleskey](#)
- [Identity Denial really exists](#)
[Roger Clarke](#)
- [Difficulties with Census Bureau income data among wealthiest](#)
[George Mannes](#)
- [Fun with stolen credit-card numbers](#)
[Jonathan Kamens](#)

● [Credit cards as ID](#)

[Ben Laurie](#)

● [REVIEW: "Intrusion Detection with Snort", Jack Koziol](#)

[Rob Slade](#)

● [Info on RISKS \(comp.risks\)](#)

✶ **Walter Cronkite: The New Inquisition**

<Dave Farber <dave@farber.net>>

Tue, 07 Oct 2003 13:58:43 -0400

[The last sentence is right on. djf]

From: CMESSALL <CMESSALL@mykotronx.com>

Walter Cronkite: "...Unfortunately, security and liberty form a zero-sum equation. The inevitable trade-off: to increase security is to decrease liberty and vice versa. In the past, such trade-offs have been temporary -- for the duration of the crisis of the moment. But today, we cannot see an end to the War on Terrorism, and that forces us to decide how secure we have to be and how free we want to be."

Wow, have we already forgotten Ben Franklin's statement: "People who are willing to trade security for freedom soon find out that they have neither."? In all fairness to Walter (who, I would have thought, might have actually *heard* Ben say those magic words ;-)), the trade-off might be correct at any given point in time, for the technology that applies at that instant. The secret of course is to change the rules (i.e., the technology)

so that we can have more security AND retain our liberty. -
Chuck Messall

IP Archives at: <http://www.interesting-people.org/archives/interesting-people/>

✉ Re: Spam abounds ([RISKS-22.92](#))

<"Peter G. Neumann" <neumann@csl.sri.com>>

Tue, 7 Oct 2003 11:16:28 PDT

Thanks to many of you who responded thoughtfully to my plaintive cries of Spam-woe. The simplest approach something that I have been contemplating for some time is to suggest that, if you want to significantly raise the probability that your message to RISKS will not be ignored, use the current string to include in the subject line. "RISKS" itself in the subject line is less than ideal, because a surprising number of spams actually include that. But for the foreseeable future, to radically improve my well-being and ability to separate the wheat from the chaff, let's try the string
notsp:
in the subject line followed by a meaningful subject, or perhaps "notsp" appended to the subject line (CASE INSENSITIVE). This pass-string will remain relatively stable unless it gets abused, in which case I will announce a phased-in change. Many thanks for putting up with this inconvenience.

Other remedies were suggested by RISKS readers (although some of them are not really suitable for RISKS-types of operations):

- * Greylisting

- <<http://projects.puremagic.com/greylisting/>>

- * Spambayes

- <<http://spambayes.sf.net>>

(following the inspiration of Graham, extensively tested and improved)

- * Indirection to a Web page that has the CURRENT valid address that

- changes as needed, plus procmail filters

- * TMDA anti-spam challenge-response software

- <<http://tmda.net>>

- * Client-side POPfile proxy (open source, cross-platform)

- <<http://popfile.sourceforge.net>>

- * Bogofilter and various other filters

- * Just change your e-mail address as often as desired, and notify your

regular communicators (clearly not applicable for RISKS, which

graciously receives e-mail from first-time contributors and needs

the stability of a permanent address).

An important concept in any such approach is that YOU should have flexible control over it, rather than some third-party who tells you what you should be willing to accept or reject. There is no one-size-fits-all. However,

- * Tripoli is a flexible approach that could help significantly.

- <<http://www.pfir.org/tripoli-overview>>

California spammin'

<"NewsScan" <newsscan@newsscan.com>>

Thu, 25 Sep 2003 06:31:25 -0700

California's new anti-spam law may face the same fate as a similar law in Utah earlier this year. Kevin Johnson of the e-mail marketing company Digital Impact warns: "Hard-core spam will still come through, but legitimate companies will be more hesitant to send e-mail"; he also warns that when companies try to determine whether e-mail recipients live in California, spammers and advertisers may be forced to learn more about consumers, thereby reducing privacy. E-mail marketer Trevor Hughes suggests that the only answer is national legislation to harmonize spam laws in more than 30 states. [*USA Today*, 24 Sep 2003; NewsScan Daily, 25 Sep 2003]

http://www.usatoday.com/tech/news/2003-09-24-spam_x.htm

Worm FAQ

<Stuart Staniford <stuart@silicondefense.com>>

Mon, 6 Oct 2003 15:34:48 -0700

I just finished a first cut at a FAQ on worms and worm containment (my obsession for the last couple of years). It may be of interest to RISKS readers:

<http://www.NetWorm.org/faq/>

Stuart Staniford, President Tel: 707-445-4355 x 15
Silicon Defense - The Cyberwar Defense Company

✶ Jury convicts man in DMCA case (Paul Festa)

<Monty Solomon <monty@roscom.com>>

Thu, 25 Sep 2003 01:51:39 -0400

Paul Festa, Staff Writer, CNET News.com, 23 Sep 2003

A federal jury has convicted a Florida man of violating the Digital Millennium Copyright Act, in the first jury-trial conviction under the controversial law, according to a U.S. attorney's office. The Los Angeles jury found 38-year-old Thomas Michael Whitehead guilty on Friday of selling hardware that could access DirecTV satellite broadcasts without paying for them, according to the U.S. attorney's office in Los Angeles. Whitehead, who was also known by his computer name "JungleMike," was convicted on one count of conspiracy, two counts of selling hardware that unlawfully decrypted the broadcasts, and three counts of violating the DMCA. With the six felony convictions, Whitehead faces up to 30 years in federal prison and fines of as much as \$2.75 million. Sentencing is scheduled for Jan. 26, 2004. ...

<http://news.com.com/2100-1025-5080807.html>

✶ Broward considers dumping \$17 million in touch voting machines

<Kim Alexander <kimalex@calvoter.org>>

Thu, 25 Sep 2003 08:39:48 -0700

Here's some good news out of Florida. Broward County is lobbying for approval of printers for touchscreens, and one of their election officials expresses regret for purchasing them in the first place. Here's an excerpt:

The touch-screen machinery accounted for part of the problems in the 2002 elections in Broward.

During the September primary, election workers found more than 1,000 votes that had not been reported in initial tallies to the state because machines had not been shut down properly. And then in the November election, officials botched the numbers by not including in the tallies ballots cast by English-speaking early voters.

"Hindsight is 20/20, but I wish we had stayed with optical scan," Commissioner Kristin Jacobs said.

Source: Broward considers dumping \$17 million in touch voting machines,

Scott Wyman, 24 Sep 2003, *South Florida Sun-Sentinel* <Sun-Sentinel.com>

Kim Alexander, President, California Voter Foundation
kimalex@calvoter.org, 916-441-2494, <http://www.calvoter.org>

⚡ Diebold voting machines in Volusia County FL

<"Brent M.P. Beleskey" <voterscoalition@rogers.com>>

Wed, 24 Sep 2003 09:57:44 -0400

ELECTION THEFT 2000! A NEW BOMBSHELL!: A Diebold Voting Machines in Volusia

County, Florida, Tallied a Vote-Count of -16,022. That's NEGATIVE 16,022:

When will this all-important story break out in the US mainstream press?

When will the Democrats confront the issue? What is at stake here is the future of democracy.

Diebold Internal Support Memos

[The original article to which this post refers was originally published on

29 Nov 2000 in *USA Today* by Philip Meyer. When I did a search for the

article on the www.usatoday.com website I came up with this page which

clearly provides the details of the article and even offers a link to a free

preview of the article. However, when you click on the link, it gives you a

page void of the article. What happened to it? One can only speculate.

Nevertheless, I have obtained the original article. BMPB]

[Contact Brent Beleskey <voterscoalition@rogers.com> for the article, PGN]

A remarkable exchange concerning Diebold's voting machines in Volusia

County, Florida: On January 17, 2001, Lana Hines, a county elections

official sends out an inquiry as to how Al Gore ended up with a vote-count

of -16,022. That's NEGATIVE 16,022 -- which just happens also to have been

the total number of votes cast for various independent and third-party

candidates who also ran. (It was the largest number of such

votes cast in
Volusia County's history.)

Pay close attention to the final entry, from "Tab" (Talbot)
Iredale,
Vice President of Research & Development at Global/Diebold:

...The error could only occur in one of four ways:

1. Corrupt memory card. This is the most likely explanation for
the problem

but since I know nothing about the 'second' memory card I have
no ability

to confirm the probability of this.

2. Invalid read from good memory card. This is unlikely since
the

candidates['] results for the race are not all read at the
same time and

the corruption was limited to a single race. There is a possib
[ility

that a section of the memory card was bad but since I do not
know anything

more about the 'second' memory card I cannot validate this.

3. Corruption of memory, whether on the host or Accu-Vote.
Again this is

unlikely due to the localization of the problem to a single
race.

4. Invalid memory card (i.e., one that should not have been
uploaded).

There is always the possib[ility that the 'second memory
card' or 'second

upload' came from an unauthorised source.

And that's only the tip of the iceberg.

Identity Denial really exists

<Roger Clarke <Roger.Clarke@xamax.com.au>>

Sat, 27 Sep 2003 11:17:22 +0800

[Admittedly this is a story from mainland China, and stories from there are often mistranslated linguistically and culturally when they reach English-language papers. But it appeared in the quality Hong Kong daily. It would seem reasonable to assume that their staff can read the original, and not make too many mistakes in the translation.]

Woman wins case against in-law for ID cancellation

A 98-year-old woman will be paid damages for psychological injury inflicted by her daughter-in-law, a Beijing court has ruled. The *Beijing Daily* reports that the elderly woman discovered her relative cancelled her identity registration card seven years ago. The defendant claims she cancelled the card to ensure her mother-in-law would not be cremated after she died. Cancelling the card made the woman non-existent in the eyes of the law.

Source: *South China Morning Post*, dateline Beijing, 26 Sep 2003
[They have a closed web-site, so I can't find the URL]

Roger Clarke <http://www.anu.edu.au/people/Roger.Clarke/> +61 2
6288 1472
Xamax Consultancy Pty Ltd, 78 Sidaway St, Chapman ACT 2611
AUSTRALIA

⚡ Difficulties with Census Bureau income data among wealthiest

<George Mannes <George.Mannes@thestreet.com>>

Tue, 7 Oct 2003 14:46:24 -0400

The Five Dumbest Things on Wall Street This Week

By George Mannes, Senior Writer, 3 Oct 2003

<http://www.thestreet.com/markets/dumbestgm/10117038.html>

[George sent RISKS an excerpt, namely, the FIRST of five dumbest things.

I had difficulty trying to abridge it for RISKS, and decided to include

it in its entirety. See the URL for the other four. PGN]

1. I Dream of the Gini Index

We at the Five Dumbest Things Research Lab hate to go all anti-academic on

you, but here's a little advice: The next time you see a statistic in the

newspaper, don't believe it. It's wrong. OK, OK. That's overstating our

case a little. It's not necessarily wrong. But it's not right, either.

Exhibit A: The 2002 household income figures released last Friday by the U.S. Census Bureau.

The takeaway from the report, as you may have read in *The Wall Street

Journal*'s Monday account, was that the poverty level rose, but income

inequality didn't, because rich folk's income took a beating, too.

But something further down in the write-up caught our eye.

"Difficulties in recording seven-figure incomes," reported the Journal, might have resulted

in underreported income among the wealthiest Americans.

In other words, the rich may be richer.

That's odd, we thought. People pay a lot of attention to these annual income-disparity figures. How come no one's getting worked up about inaccurate data from such a key segment of the surveyed population? This can't be true.

We called up Edward Welniak, chief of the Census Bureau's income survey, to check.

Indeed, there are difficulties with high-income data, Welniak told us.

Here's why: Starting with the 1993 numbers, the bureau's staff -- which interviews a sample of 78,000 households for the income survey either in person or over the phone -- has been entering people's responses directly into portable or desktop PCs. As part of the survey, respondents are asked to report how much money they made the previous year from numerous sources -- stuff like the job held the longest, interest and dividends.

And here's the catch: In each category, the highest dollar amount one can enter is \$999,999.

So let's say a Census employee had dropped by the \$15,000-umbrella-stand-festooned apartment of ousted Tyco Chairman Dennis Kozlowski in 2001. And let's say the then-executive wanted to report the \$50 million or so in undisclosed compensation the Securities and Exchange Commission says he received in 2000.

Well, Kozlowski couldn't have done it. The Census would have

recorded his salary at a mere million bucks.

"The fact that we're not recording the full dollar value is going to understate the share of income controlled by households at the highest levels," says Welniak.

But, says Welniak, there's a good reason for capping monetary entries at six digits: It limits the potential for error. One extra digit at the high end, and you're talking about, say, a \$9 million paycheck instead of a \$900,000 payout. Errors at the high end of the income scale have a much larger impact than errors at the bottom. The increased accuracy introduced by more possible digits, says Welniak, would be more than offset by the decreased accuracy from newly enabled errors.

Welniak has even investigated the exact effect of rounding all multimillion-dollar income sources down to a megabuck. According to his analysis of numbers from 1999 -- a year for which 26 respondents reported employment compensation of at least \$1 million in at least one category -- data-entry limitations effectively understated income inequality by 1%, using a standard measure of income distribution known as the Gini Index.

But, given that the error appears to be constant year after year, says Welniak, "Measuring changes in income inequality from one year to the next is not going to be affected." In other words, ignore the absolute number and look at the trend.

Mindful of that, we point out that over the past decade, the Census Bureau's Gini Index has been creeping upward -- implying increased income inequality. Starting at 45.4 in 1993, it peaked at 46.6 in 2001 but retreated to 46.2 last year. (For purposes of comparison, the United Nations Development Program -- which puts the U.S. at 40.8 -- says Japan is a 24.9 and Brazil is a 60.7.)

In fact, someone has gotten worked up about the low-balled high incomes: the Center on Budget and Policy Priorities, a D.C.-based research group. The CBPP has been complaining about the Census data for years, griping not only about the \$999,999 cap but also about the Bureau's exclusion of capital gains from household income.

"The census data has useful information," says Isaac Shapiro, a CBPP senior fellow. "But at the high end, it's not useful."

Based on Congressional Budget Office data, the CBPP says the average household after-tax income in the top 1% of the population tripled from \$286,000 in 1979 to \$863,000 in 2000, while the lowest fifth of the population saw household income rise a mere \$1,100 to \$13,700 over the same time period.

Put that in your Gini Index and smoke it.

George Mannes, 14 Wall Street - 15th Floor / New York, NY 10005
phone: 212-321-5208 / mobile: 646-641-2093

<http://find.thestreet.com/cgi-bin/teaxis/author/?au=A0000332>

✶ Fun with stolen credit-card numbers

<Jonathan Kamens <jik@kamens.brookline.ma.us>>

Fri, 5 Sep 2003 11:31:57 -0400

Yesterday, I got an e-mail message from Amazon.com which I am including here

in full (word wrapped and with some details obscured but otherwise

unmodified) because I believe it will be of interest to RISKS readers.

Additional comments from me follow the message.

X-AMAZON-TRACK: <jik@kamens.brookline.ma.us>

Date: Thu, 4 Sep 2003 16:01:07 -0700

From: charge-inquiries@amazon.com

To: jik@kamens.brookline.ma.us

Cc: charge-inquiries@amazon.com

Subject: Your Credit Card Account

Greetings from Amazon.com.

We perform routine reviews of orders to protect our customers. During one

of these reviews we discovered that an account was opened with a card used

by you on another account. For your reference the card in question is a

American Express card with the last five digits of [deleted].

As it appears the card was used without your authorization, we have closed

this new account and cancelled any outstanding orders. If the account is

indeed yours, we apologize for any inconvenience caused and ask that you

notify us by replying to this email message as soon as possible. If the

card was used without your authorization, we recommend you cancel the card

immediately by contacting the financial institution that

issued the card.

Unfortunately, if this is the situation, you should know that a charge in the amount of \$556.94 was processed by us.

You should review all recent charges made to this card, reporting any unauthorized charges, including those mentioned above, to your financial institution. The financial institution, in turn, will send you forms to formally dispute the unauthorized charges, the applicable merchants will be notified and charged back, and your account subsequently credited. Additionally, you may wish to report this matter to the applicable law enforcement agency.

We were able to verify that your card was not compromised from our site.

Our credit and debit card data is stored on a computer that is not connected to the Internet. When data is received it is sent to a dedicated computer via a proprietary one-way interface across a simple serial connection. The information is stored no other place, access to the data is restricted and, when accessed, logged.

Although we are not permitted to provide you with any details about the unauthorized use, we will provide this information to any law enforcement agency investigating this matter as well as to the financial institution.

Please don't hesitate to contact us if you have any further questions or concerns.

Sincerely,

Ben
Investigation Specialist
Amazon.com
<http://www.amazon.com>
Earth's Biggest Selection
=====

I went to the American Express Web site and checked the unbilled activity on the card, and, indeed, found a charge of \$556.94 to Amazon.com on August 31 which I did not make. I also found another charge I did not make of over \$500 to Amazon.com on August 27.

I called the telephone number on the back of my card, navigated through voice-mail for several minutes and then spoke to three representatives. The first deactivated my card, issued me a new one, and transferred me to the customer service department. The customer service rep transferred me to the fraud department. The fraud rep ask me a few questions that were probably from a script ("Was your card ever out of your possession?" "Did you make these charges?", etc.). Then she said that the charges would be removed from my account and investigated.

Some things here worked very well. It's good that Amazon caught the bogus charges relatively quickly and notified me about them. It's good that American Express was polite and was able to deactivate my card, issue me a new one, and remove the bogus charges from my account quickly.

Some things did not work so well. Why didn't Amazon stop the perpetrators in real-time from making a purchase using a card already registered to

another account, as opposed to only detecting the situation after the fact?

Since I assume that the fraudulent purchase was shipped to an address other

than mine, why didn't Amazon require additional verification before shipping

over \$500 of merchandise to an address other than the card's billing

address?

There are some questions whose answers I do not know, and neither Amazon nor

American Express is telling. Did the perpetrator use my name?

Did s/he

know my correct billing address? Did s/he know the security code printed on

the front of the card? And if the answer to any of these questions is "no,"

why did Amazon allow the charge? And the biggest question, to which I'll

probably never know the answer, is, how did the perpetrator steal my info?

Even if they catch him/her and find out, it's unlikely that the information

will trickle back to me.

Today I'll be contacting all the credit-reporting agencies to put a fraud

alert on my report and ask them for free copies so that I can verify that

this is merely a case of isolated credit-card number fraud as opposed to

full-scale identity theft. Who knows, this may be the start of a very bumpy

ride.

Jonathan Kamens

Credit cards as ID

<Ben Laurie <ben@algroup.co.uk>>

Fri, 03 Oct 2003 12:50:21 +0100

About a week ago, our front door was broken down at 3 in the morning. The burglars took my wife's handbag from the hall and ran (luckily, it didn't contain her car keys, because a common strategy is to return in a few hours and take the car, too).

Today, we received a number of phone contracts. These may or may not have been paid for with the stolen credit cards [1], but (we are informed) the credit cards were used for ID.

This got me thinking. My credit cards are often used for ID, too. But they never check whether the card has been stolen - all they check is that it has the right name on it.

Now, given that the most common case of this occurring is when I take internal flights in the UK, I'm suddenly worried. The risk is obvious.

Incidentally, the incidents also show the lack of value of photo ID - at least one of the contracts requires proof of address, and the only proof in the handbag was my wife's driving licence. Which has a photo on it. So I guess we can add that as a second risk (i.e. relying on photo IDs for fraud prevention).

[1] Since my wife spent the time waiting for the police cancelling all her cards, they may not have been used.

<http://www.apache-ssl.org/ben.html>
[net/](http://www.apache-ssl.org/ben.html)

<http://www.thebunker.net/>

REVIEW: "Intrusion Detection with Snort", Jack Koziol

<Rob Slade <rslade@sprint.ca>>

Mon, 6 Oct 2003 21:22:12 -0800

BKINDTSN.RVW 20030901

"Intrusion Detection with Snort", Jack Koziol, 2003, 1-57870-281-X,

U\$45.00/C\$69.99/UK#32.99

%A Jack Koziol

%C 201 W. 103rd Street, Indianapolis, IN 46290

%D 2003

%G 1-57870-281-X

%I Macmillan Computer Publishing (MCP)

%O U\$45.00/C\$69.99/UK#32.99 800-858-7674 info@mcp.com

%O <http://www.amazon.com/exec/obidos/ASIN/157870281X/>

robsladesinterne

<http://www.amazon.co.uk/exec/obidos/ASIN/157870281X/>

robsladesinte-21

%O <http://www.amazon.ca/exec/obidos/ASIN/157870281X/>

robsladesin03-20

%P 340 p.

%T "Intrusion Detection with Snort"

Chapter one is a good introduction to the basics of intrusion detection, although it is odd that the list of detection methods is missing some important entries, such as heuristic rule-based and statistical methods.

The background overview of Snort, in chapter two, describes alerts, related applications, and even has recommendations for sensor net architecture.

Most of the content in regard to the components of Snort, in chapter three, deals with the preprocessors, and various attack signatures. Chapter four's advice about planning for the installation of Snort is broadly based, addressing policy, architecture, and even incident response, but the material is quite abstract, and could have benefitted from more practical examples. Some of these missing considerations are dealt with in chapter five, which looks at hardware and operating system factors. The text concentrates on server and sensor performance, but also addresses the network connection. Directions on building a Snort server under Red Hat Linux version 7.3 are given in chapter six. The sensor and console instructions are provided in chapters seven and eight, respectively. A few optional architectures are described in chapter nine.

Chapter ten deals with tuning various rulesets and components in order to reduce the level of false alarms. Creating real-time alert systems is discussed in chapter eleven. Chapter twelve is a major one, outlining the creation and modification of rules for filtering and analyzing traffic. Chapter thirteen is supposed to be about upgrading and maintaining Snort, but concentrates on ancillary management tools. Advanced or unusual configurations of Snort are described in chapter fourteen.

The book is generally lucidly written and easy to study, but it contains many typographical errors and a great deal of clumsy wording in the text. Better copy editing would have improved readability, as well as

confidence in
the reliability of various commands and settings. However, the
meaning is
usually clear, even if the expression is sometimes jarring. For
those
planning to use Snort, this should be a serviceable introduction.

copyright Robert M. Slade, 2003 BKINDTSN.RVW 20030901
rslade@vcn.bc.ca slade@victoria.tc.ca rslade@sun.soci.
niu.edu
<http://victoria.tc.ca/techrev> or [http://sun.soci.niu.edu/
~rslade](http://sun.soci.niu.edu/~rslade)



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

[ACM](#) Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 94

Thursday 9 October 2003

Contents

- [Analysis of California recall data confirms voting system doubts](#)
[Rebecca Mercuri via PGN](#)
- [Faulty wiring led to windshield cracks in 3 Boeing 777s](#)
[Monty Solomon](#)
- [The Earth's not slowing down fast enough to suit Motorola](#)
[Paul Eggert](#)
- [German toll system unusable](#)
[Debora Weber-Wulff](#)
- [School district sued over WLAN planning](#)
[Monty Solomon](#)
- [Risk of trusting computer-free security?](#)
[George Mannes](#)
- [Telephone evidence vs. armed robbers](#)
[Roger Willcocks](#)
- [New CD antipiracy mechanism disabled by shift key](#)
[Joshua Levy](#)
- [Re: Parking chaos in York](#)
[Chris Barnabo](#)
- [Re: A new approach to roller coasters](#)
[Lars-Henrik Eriksson](#)

- [Franklin security/liberty quote](#)
[Duke Robillard](#)
 - [Re: Fun with stolen credit-card numbers](#)
[Dimitri Maziuk](#)
 - [Re: Unencrypted credit-card submission forms](#)
[Ben Scott](#)
 - [Getting over that fishbowl feeling: harvested data](#)
[Rick Smith](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✂ Analysis of California recall data confirms voting system doubts

<"Peter G. Neumann" <neumann@csl.sri.com>>

Thu, 09 Oct 2003 07:10:04 -0400

(from Rebecca Mercuri)

Following is based on information from Rebecca Mercuri.
[The words are hers, not mine, lightly edited for RISKS.]

Rebecca Mercuri has analyzed California's recall ballot data and reports that it confirms numerous doubts about election systems. Her results demonstrate that the style of voting system in use (punchcard, optically scanned, or touchscreen) cannot be generically considered either "good or bad". She asserts that the particular model of the system, as well as the procedural controls in place in each county, along with the ballot layout, may have considerably more impact on the reliability of the election results than the type of system deployed.

The analysis revealed some shocking details. Of the 8,359,168 votes cast statewide, some 384,427 (nearly 4.6%) were not recorded for the

recall

question. Almost half of these missing votes (over 175,000) were in Los Angeles, nearly 9% for that county. Yet the Datavote punchcards used in 14 other counties fared somewhat better, on average, than all of the optically scanned and touchscreen systems, with the exception of only the ES&S Optech Eagle (used in San Francisco and San Mateo counties) and the Diebold Accu-Vote-TS (used in Alameda, though with some reports of equipment malfunctions). The Sequoia Edge touchscreens, currently under litigation in Riverside County, performed slightly worse than the Datavote punchcards. The ES&S iVotronic touchscreens were ranked lowest of the three touchscreen types in the state, and were outperformed by all other systems with the exception of the Sequoia Optech optically scanned systems and the Pollstar and Votomatic punchcards.

In earlier court battles prior to the recall election, the ACLU claimed that voters using punchcards would be unfairly disenfranchised, as compared to voters using optically scanned or touchscreen systems. As it turns out, the counties using Datavote punchcards had residual vote rates that were better than all but one of the optically scanned systems, and also lower than two of the three touchscreen systems. At the other end of the scale, the counties using Pollstar and Votomatic punchcards (which included heavily-populated Los Angeles) had worse residual vote rates than any other type of voting system in use in the state. Clearly it is not the punchcards themselves that are to blame, since the Datavote systems

demonstrate that
punchcards can be used successfully.

The residual vote technique was previously used by MIT/Caltech in their studies following the 2000 Presidential Election. For the California analysis, she performed her calculations by comparing the difference between the total number of ballots cast, as reported by California Secretary of State Kevin Shelley's office, with the total numbers of "yes" and "no" votes on the recall question. It should be noted that the residual vote tally is incapable of differentiating between a voter who deliberately or accidentally did not make a selection on the recall question, and an equipment failure (such as hanging chad) that could result in a cast vote not being counted.

The rush to fully computerized ballot casting is misguided. Although supplemental technologies are needed for disabled voters, there is no clear evidence that touchscreen systems are substantially or consistently better for use by the general population than other voting methods. The fact that the touchscreens in California do not provide any way to perform an independent recount [and no real assurance that votes are even handled correctly in the absence of the voter-verified audit trail that Rebecca has long been recommending -- PGN] should make them less desirable than the paper-based systems that do have such capabilities. Counties, like San Francisco, that are doing well with optically scanned ballots, and the smaller ones that use punchcards effectively, should feel no

pressure to
modernize.

For further information, contact Rebecca Mercuri via telephone at
1-609/895-1375 or 1-215/327-7105, email mercuri@acm.org and
Internet at
<http://www.notablesoftware.com/evote.html>

-- -- -- --

Supporting Data for California Recall Question, Rebecca Mercuri
7 Oct 2003

Numbers represent RESIDUAL VOTE RATE as percentage of total
votes cast
according to type or model of machine:

Punchcard	6.24
Datavote	1.94
Pollstar	6.02
Votomatic	8.17
Optically Scanned	2.68
ES&S Eagle	1.87
Diebold Accu-Vote-OS	2.36
ES&S 550 and 560	2.42
Mark-A-Vote	3.04
Sequoia Optech	4.35
Touchscreen	1.49
Diebold Accu-Vote-TS	0.72
Sequoia Edge	2.01
ES&S iVotronic	3.49
Statewide	4.59

✶ Faulty wiring led to windshield cracks in 3 Boeing 777s

<Monty Solomon <monty@roscom.com>>
Mon, 6 Oct 2003 23:47:56 -0400

Faulty wiring in a window heater caused the windshield to crack on a Boeing 777 during a flight from Rome to New York in July 2003, and at least two other Boeing 777s have experienced similar problems in the past year, the Associated Press has learned. All landed safely and no one was hurt. But experts say three similar incidents in one year is unusual for an aircraft.

... [Source: AP, 6 October 2003]

<http://finance.lycos.com/qc/news/story.aspx?story=35949554>

[See also: 3 Windshields Cracked on Boeing 777s, Leslie Miller, Associated Press, 6 Oct 2003]

<http://finance.lycos.com/qc/news/story.aspx?story=35948868>

✶ The Earth's not slowing down fast enough to suit Motorola

<Paul Eggert <eggert@CS.UCLA.EDU>>

Tue, 07 Oct 2003 23:33:45 -0700

Motorola reports that several GPS receivers in its Oncore line will misdisplay the date on 28 Nov 2003 at midnight UTC. For a one-second window the receivers will mistakenly report the date as 29 Nov instead of 28 Nov.

Here's why. Every couple of years or so for the past three decades, the International Earth Rotation Service has announced a leap-second because the Earth is rotating slightly more slowly than an 86400-second day would suggest. But since 1 Jan 1999, we've had an unusually long dry

spell

without any leap seconds. The GPS week number in the UTC correction parameter is 8 bits long, which allows for 256 weeks of unambiguous time calculation. Until now this parameter has never rolled over, but because of the dry spell 28 Nov will be exactly 256 weeks after the most recent leap second, and the rollover will contribute to the bug.

<http://www.motorola.com/ies/GPS/docs_pdf/notification_oncore.pdf>

Steve Allen writes in <<http://www.ucolick.org/~sla/leapsecs/onlinebib.html>>

that some JDAM smart bombs and other munitions are rumored to contain these receivers. Anyone intending to use those weapons around the magic window might want to reschedule their bombing runs for some other time. ...

German toll system unusable

<Debra Weber-Wulff <weberwu@fhtw-berlin.de>>

Thu, 09 Oct 2003 20:25:05 +0200

A German consortium called TollCollect, consisting of global players such as the Deutsche Telekom and DaimlerChrysler has been trying for some time to create a "modern toll collection system" using GPS, among other things. The German Government decided today to postpone the introduction of the system, at a cost of millions of Euros, because it doesn't work.

It was to be fully automatic. Trucks (and only trucks were to

pay the toll)
were to have an OBU (On-Board Unit, and of course a different one than all the other countries using such devices. Some trucks would need 3-5 of the things, depending on the routes they take). The OBU is to have a GPS receiver and a mobile transmitter, so that when the truck is moving it's position can be determined. When the truck drives over highways that are not toll-free for trucks, the toll is to be calculated and sent by mobile transmitter to a central office, that bills the shipping company direct.

Sounds simple, doesn't it?

For this purpose, lots of new masts were erected (as if we don't already have enough of this nonsense in Germany), and a beta test was arranged. Shipping companies complained that they were charged toll, although they were using the non-toll road that ran near a toll road. [GPS tolerance miscalculated? Maybe the German mapmakers made some mistakes?]. Others reported happily that they were charged no toll, although they were using a toll road. Some truckers reported the OBU busting its circuit breakers when the ignition in the truck was started.

The problem is, that no one knows what the cause for the problems is. Maybe it is the map update system, which updates the map in the OBU about 500-1000 times a month [that is around once an hour, or more, according to my calculations! - dww]. And of course, the OBUs can't be produced fast enough so that all the trucks that cross Germany have one by 1 Nov, the

date

(already moved before) the toll was to have gone into effect.

Foreign truckers were to use a special system of 3500 terminals that are installed at truck stops throughout Germany. Or, toll could be paid in advance "by Internet". Reports are, that this doesn't work, either, and takes an enormous amount of time.

The minister for transport, Manfred Stolpe, has often been asked why German didn't use a low-tech system like Austria (they sell little stickers called Vignettes) or Italy (they put people in toll booths at specific points on the highways). Stolpe says, he wanted a high-tech solution that would work for decades.

Perhaps using a current mobile technology and old-fashioned notions of high-tech was not really a great idea? Germany has now sunk over 730 Million Euros into the project. The toll of 12.4 (euro)cents per kilometer was to bring in 2.8 billion Euros a year into cash-strapped Germany, with the consortium raking in a fifth of the take.

There has also been scandal from the get-go in 2001, where by amazing coincidence a German-led consortium won the bid, although other bidders could show that they had experience in actually building such a thing. And then the government gave them a special liability dispensation, so that the consortium doesn't have to pay a fine for missing the start date, which has been moved before.

So here we have a fine mixture of mismanagement, high-tech woes and government games. The EU in Brussels is beginning to sniff into the affair, as it is beginning to smell like fish left on the counter for a week.

At least it gives Germans something to complain about to take their minds off the unemployment figures!

[German language articles:]

http://www.tagesschau.de/thema/0,1186,OID2318248_REF1_NAVSPM1,00

Prof. Dr. Debora Weber-Wulff, FHTW Berlin, FB 4, Treskowallee 8, 10313 Berlin
Tel: +49-30-5019-2320 <http://www.f4.fhtw-berlin.de/people/weberwu/>

⚡ School district sued over WLAN planning

<Monty Solomon <monty@roscom.com>>
Tue, 7 Oct 2003 01:38:16 -0400

A school district is sued in Illinois over planning a WLAN without addressing a group of parents' concerns over electromagnetic radiation's effects.

<http://wifinetnews.com/archives/002303.html>

⚡ Risk of trusting computer-free security?

<George Mannes <George.Mannes@thestreet.com>>

Wed, 8 Oct 2003 21:08:02 -0400

A dog trainer was sentenced to 6 1/2 years in prison Monday for providing defective bomb-sniffing dogs to the government after the 11 Sep 2001 attacks and lying about their credentials. Russell Lee Ebersole, convicted in June 2003 on 27 counts of fraud, insisted his dogs were competent and blamed his conviction on jealous competitors. ... Ebersole's Detector Dogs Against Drugs and Explosives, of Stephenson, Va., provided bomb-sniffing dogs to several federal agencies in the months after the 9/11 attacks. The agencies paid Ebersole \$700,000 from Sep 2001 to May 2002. Ebersole's contracts were canceled after his dogs failed independent tests on five different occasions. On one test, dogs were unable to detect 50 pounds of dynamite and 15 pounds of C-4 plastic explosives hidden at the Federal Reserve parking garage in Washington.

[Source: Man Jailed for Faulty Bomb-Sniffing Dogs, By Matt Barakat,

Associated Press 8 Sep 2003]

[http://www.newsday.com/news/nationworld/nation/wire/](http://www.newsday.com/news/nationworld/nation/wire/sns-ap-dogs-cant-sniff,0,4930607.story?coll=sns-ap-nation-headlines)

[sns-ap-dogs-cant-sniff,0,4930607.story?coll=sns-ap-nation-headlines](http://www.newsday.com/news/nationworld/nation/wire/sns-ap-dogs-cant-sniff,0,4930607.story?coll=sns-ap-nation-headlines)

After years of reading RISKS, I have become instinctively suspicious of all the things that can go wrong in security -- and other areas -- if one trusts a computer too much. But, as this story taught me, my wariness around computers creates a new Risk: the belief that excluding a computer from a particular situation makes that situation inherently less Risky.

Before I read this, if someone had asked me what was more reliable -- a bomb-sniffing dog or a bomb-sniffing electronic device -- I'm sure I would have said the dog. What's more honest, sincere and trustworthy than a dog? Plus, from Risks I've learned that there's a huge difference between a shiny gadget's performance in a lab under controlled conditions in a lab and its performance out in the field under less orderly conditions. Unfortunately, it appears, dogs can be programmed just as poorly as computers are. - GM

[But are the high-tech systems really better than the canine sniffers?

Some of the system technologies seem to have "gone to the dogs". PGN]

🔥 Telephone evidence vs. armed robbers

<"Roger Willcocks" <roger@rops.org>>

Wed, 8 Oct 2003 16:34:26 +0100

'A gang of armed robbers collected 1.4-million pounds (UK) as they targeted the wealthy across London. The gang took all the precautions to avoid detection. Cars were stolen, laid up for a few days to make sure they had not been fitted with tracking devices, and then used. The gang wore gloves in addition to masks and balaclavas. As a result police were left without forensic evidence. But those said to be involved reckoned without the ability of telecom experts to link their use of mobiles to the

areas where
the robberies took place. "Telephone evidence is at the heart
of this case"
[the prosecution] told the jury.' [Source: *The Times*
(London), 8 Oct 2003
(abridged)]

It's been noted previously how handy it is that 'bad people'
willingly carry
tracking devices. I hope the police already had suspects and
used the phone
evidence to back up their case. The risk is that they could
trawl phone
records for correlations and suspect anybody who happened to be
in the wrong
place(s) at the wrong time(s).

⚡ New CD antipiracy mechanism disabled by shift key

<Joshua Levy <levy@csl.sri.com>>
Thu, 09 Oct 2003 11:34:09 -0700

A new and humorous approach to audio CD copy protection is based
on the
Windows feature that auto-runs code on CDs when they are
inserted. A
Princeton student has pointed out that the feature is disabled
by holding
down the shift key when inserting the disc.

http://rss.com.com/2100-1025_3-5087875.html

A satirical, but entirely too believable, take on this:

Keyboard Manufacturers Named in DMCA Suit
German-based media giant Bertelsmann Group has launched a 400
million
dollar lawsuit against major hardware manufacturers, alleging

they traffic

in banned circumvention devices that can be used to illegally copy their

music CDs. It says that the Digital Millennium Copyright Act entitles it

to protection from devices that can be used to circumvent its technological protections against piracy. Specifically, it demands

compensation for the inclusion of "Shift" buttons on standard computer

keyboards.

<http://www.kuro5hin.org/story/2003/10/8/201119/758>

⚡ Re: Parking chaos in York ([RISKS-22.92](#))

<"Chris Barnabo" <chris@spagnet.com>>

Mon, 6 Oct 2003 19:53:37 -0400

Hmmm, tough one ... how about a POWER SWITCH? For a flaky 1.5M pound system

you'd think they could throw in a few toggle switches gratis.

["Switches would be the icing on a flaky 1.5M pound cake" ...]

<http://www.spagnet.com>

⚡ Re: A new approach to roller coasters (Baker, [RISKS-22.89](#))

<Lars-Henrik Eriksson <lhe@csd.uu.se>>

Thu, 9 Oct 2003 09:28:30 +0200

I have actually tried this thing and it is not apparent that Windows is

controlling the RoboCoasters. The programming is certainly done on a touch-screen PC, but the program is delivered to the visitor on a smart card. The smart card is then inserted into the RoboCoaster's control system, which looks like a traditional industrial process control system -- e.g. no screen, but lots of lights and buttons.

To me this looks like a prudent way of separating the programming and control systems which have very different user interface and safety requirements.

Lars-Henrik Eriksson, Computing Science, Dept. of Information Technology,
Uppsala University, Sweden <http://www.csd.uu.se/~lhe> +46 18
471 10 57

✶ Franklin security/liberty quote (Re: Cronkite: The New Inquisition)

<Duke Robillard <duke@io.com>>
Wed, 08 Oct 2003 10:40:35 -0400

Old Ben wasn't quite **that** radical. :-) What he actually wrote was

They that can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety

Historical Review of Pennsylvania, 1759 (although he used it earlier in a letter; cf. <http://www.bartleby.com/100/245.1.html>)

I think the Ben's choice of words makes his meaning quite different than your's. In particular, Ben says they "deserve neither," not that they'll "have neither." He's making a value judgment, saying that "essential liberties" are intrinsically better than "temporary securities," and that people who disagree don't deserve either. You're saying that giving up liberty will mean you can't get security. That argument could be made, but Ben wasn't making it in this quote.

Ben's original quote also gives the Patriot Act guys plenty of wiggle room, by using the phrases "essential liberty" and "temporary safety." Who's to judge "essential" and "temporary"?

⚡ Re: Fun with stolen credit-card numbers (Kamens, [RISKS-22.93](#))

<dmaziuk@bmr.b.wisc.edu (Dimitri Maziuk)>

Wed, 8 Oct 2003 19:07:15 -0500

Jonathan Kamens:

> Subject: Fun with stolen credit-card numbers

(OP re-formatted)

> There are some questions whose answers I do not know, and neither Amazon nor

> American Express is telling. Did the perpetrator use my name? Did s/he

> know my correct billing address?

A bank generally doesn't care about these. You put card number and

transaction amount into EFT terminal and get a response sometime later,
that's all. Response is a success or error code. And they don't really care about expiry date, either: you get a different error code for expired card.

The number uniquely identifies a current account (I don't know if they guarantee that numbers will never get re-used). It does not identify the actual card: my wife and I have credit cards with the same number.

There's no such thing as billing address for credit cards -- as far as bank is concerned.

It gets better: my wife kept her maiden name. She is currently working at one university while I am working at another, in a different state. She has a different billing and shipping addresses, in addition to different name -- and the same credit-card number.

So the vendor has no a priori means of deciding if the same credit card number may or may not be used with different name and/or address(es). They have 2 choices: 1) block legitimate purchases and drive off potential customers. In other words, what's not explicitly allowed is forbidden (totalitarian). PayPal does that -- account owner has to add the other cardholder to the account before PayPal will let them pay for anything.

Or 2) let the transaction through and notify the cardholder so they can decide whether the transaction was indeed fraudulent. IOW, what's not

explicitly forbidden is allowed (democratic). Since credit card issuers will usually reverse fraudulent charges at your say-so, there's little harm to the customer.

> Since I assume that the fraudulent purchase was shipped to an address other
> than mine, why didn't Amazon require additional verification before shipping
> over \$500 of merchandise to an address other than the card's billing
> address?

Because some people may be buying presents for others and have them shipped directly to the recipient, for one thing.

> Some things did not work so well. Why didn't Amazon stop the perpetrators
> in real-time from making a purchase using a card already registered to
> another account, as opposed to only detecting the situation after the fact?

Probably because Amazon doesn't lose enough to fraudulent purchases, so they're more concerned with making customer's life easier. Otherwise they'd go for totalitarian option.

Credit card issuers do the same thing. Credit cards weren't designed to be secure, that's where the problem really is. But nobody's rushing to fix the system (unless you count another little number printed on the same piece of plastic -- well, on some of them anyway -- as a fix). Presumably because that'd be more expensive than just reversing transactions whenever someone tells them to.

✦ Re: Unencrypted credit-card submission forms (Silverberg, [RISKS-22.92](#))

<Ben Scott>

Thu, 09 Oct 2003 11:50:41 -0700

My soon-to-be former web hosting company (name omitted until I can migrate my sites away from them, but it rhymes with "LinuxWebToast dot com"...) has a billing page which invites you to submit credit-card info, unencrypted. When you click on a tiny link to "Access this page securely", a browser security warning pops up - the certificate shows a company name of "SnakeOil Ltd" (which I understand is a sample included with many webserver software packages for testing purposes), and it's been expired since October 2001! I only discovered this when I tried to change the credit card I've been using for years; the company has ignored repeated requests for an explanation, though they're pretty prompt about responding to any other query...

✦ Getting over that fishbowl feeling: harvested data

<Rick Smith <smith@smat.us>>

Thu, 09 Oct 2003 08:51:12 -0500

I was at Black Hat last week during which Lance Spitzer talked about hacker community activities he's been seeing. One comment that really

caught my interest was his claim that today's typical hacker is actually in it for the money: there's something to be gained by harvesting legal e-mail addresses to sell to spammers and by harvesting credit-card data. And I mean *harvest*. Individual addresses and numbers aren't worth much by themselves.

Spitzer also claimed that at this point the financial community assumes that all relevant credit-card numbers and personal information for all their customers has probably been captured by someone in the hacker community. The only reason one person or another hasn't been hit is because there are more potential targets out there than the perpetrators have time to attack.

A piece of evidence he presented to support this was a set of estimates of the street value of ID information: \$1 for a valid card number, \$5-10 for one with personal info to back it up (name, addr, etc), and \$10-15 if it includes the CVV2 number from the back (amounts are quoted from my notes). In short, it's a "buyers market" for credit-card info.

One plausible use of all these exploitable card numbers is a variant of "salami slicing:" you systematically remove a small, plausible amount of money from a victims' account. I've seen two instances on our accounts, one apparently for "AT&T" phone and one for a "Columbia House" club. The charges seemed plausible because my daughter was at school and had been given permission to pay for such things.

Moreover, the legitimate charges appeared on different credit-card bills from the illegitimate ones. Charges looked plausible when looking at bills individually. We only tracked it down when we compared monthly expenses across all the bills. This is an example of why even three or four credit cards may be too many to own.

The credit-card companies did a fairly thorough job of reversing the charges, but I suspect the losses are still too small to expect that anyone will go after the perpetrators.

Rick Smith, University of St. Thomas/Cryptosmith,
rick@cryptosmith.com



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 95

Friday 10 October 2003

Contents

- [New breed of 'spackers' eludes antispammers](#)
[NewsScan](#)
- [OCLC ILL System's rolls over 130th time...](#)
[Brig C. McCoy](#)
- [SunnComm: DCMA strikes again](#)
[Peter Houppermans](#)
- [SunnComm won't sue Princeton student over "shift key" paper](#)
[Declan McCullagh](#)
- [Microsoft to fix Windows -- again](#)
[Gene Lambson](#)
- [Winning the security trifecta](#)
[Jeremy Epstein](#)
- [Something's fishy with Diebold in California](#)
[Craig DeForest](#)
- [Data transfer Excel-COBOL loses voter data](#)
[Patrick O'Beirne](#)
- [The shape of elections to come in England](#)
[C. Cartledge](#)
- [Risks of living in New Mexico](#)
[Kent Hartfield](#)

- [Re: Unencrypted credit-card submission forms](#)
[Jeffrey W. Baker](#)
 - [Re: Hidden risks: location dependence](#)
[Mark Brader](#)
 - [Re: Identity Denial really exists](#)
[Paul Wallich](#)
 - [Re: Too much spam filtering](#)
[John Bechtel](#)
 - [Observed sudden 1400-fold increase in W32/Swen infected e-mails](#)
[Jon Seymour](#)
 - [Re: Difficulties with Census Bureau income data](#)
[Tony Lima](#)
 - [Re: Getting over that fishbowl feeling](#)
[Identity withheld](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✶ **New breed of 'spackers' eludes antispammers**

<"NewsScan" <newsscan@newsscan.com>>

Thu, 09 Oct 2003 09:35:20 -0700

Computer crackers have joined forces with spammers to devise new ways of defrauding hapless Internet users. The latest technique enables spammers to create Web sites that are virtually untraceable, making it impossible for antispammers to shut down those sites by conventional means. Typical of the scam is a group in Poland currently advertising "invisible bulletproof hosting" for \$1,500 a month, which provides its clients protection from network sleuthing tools such as 'traceroute' and 'whois' by routing traffic through thousands of hijacked computers (most of them home computers running

Windows and having broadband connections). The technique is effective.

"You're not going to have much success trying to follow IP addresses through hacked hosts," says one security researcher. "About all you can do is follow the money -- sign up for whatever it is they're selling and try to figure out who's behind the whole thing." Fueling the new tactics is an influx of "engineers who have been laid off or fired, and people who really know what they're doing with networking and DNS," says Steve Linford, head of the Spamhaus Project. "Hackers used to detest spammers, but now that spamming has become such a big business, it's suddenly cool to be a spammer."

[Wired.com 9 Oct 2003; NewsScan Daily, 9 Oct 2003]

<http://www.wired.com/news/business/0,1367,60747,00.html>

✶ OCLC ILL System's rolls over 130th time...

<"Brig C. McCoy" <brigc@world.std.com>>

Fri, 10 Oct 2003 15:38:34 -0500

The OCLC (Online Computer Library Center) Interlibrary Loan System is used by many libraries around the world to facilitate interlibrary loan of materials.

Unfortunately, the system display only shows record numbers up to 999999.

This means that, with OCLC ILL transaction 130,000,000 due to happen in a few days, they will have rolled over 130 times without changing

the system
to allow for an appropriate number of digits!

Brig C. McCoy, 4722 Oak St, Apt 1033, Kansas City, MO 64112
<<http://www.theworld.com/~brigc>> 1-816 885-2700 <BRIGC@WORLD.
STD.COM>

✶ SunnComm: DCMA strikes again

<Peter Houppermans <peter.houppermans@paconsulting.com>>
Fri, 10 Oct 2003 07:17:58 +0100

If I buy a doorlock I'd be jolly grateful to find out that it
takes hairpin
+ primary school kid to brake it (and I'd be rather annoyed with
the
supplier). But instead of said supplier fixing the problem -
you guessed
it, they go and sue the person who told the world.

Same with SunnComm: a student discovers a simple bypass for
their heavily
marketed "CD" protection - and hey, new, surprising move: they
sue.

Register article "SunnComm to sue 'Shift key' student for \$10m",
URL
<http://theregister.co.uk/content/6/33322.html>

Question: is this really the best way to rescue your reputation?
Answer: if you want to create the impression that you don't want
to fix the
problem you couldn't have chosen a better route.

The longer I've been on the RISKS list, the more convinced I
become the DCMA
is a serious threat to security. I'd like to hear of examples
where it has

contributed to actual security rather than allow security through obscurity to prolong its life ..

Peter Houppermans, PA Consulting Group, 123 Buckingham Palace Road
London SW1W 9SR +44 (0)20 7333 5303 <http://www.paconsulting.com>

✶ SunnComm won't sue Princeton student over "shift key" paper

<Declan McCullagh <declan@well.com>>
Fri, 10 Oct 2003 14:25:01 -0400

SunnComm won't sue grad student, By Declan McCullagh, 10 Oct 2003
<http://news.com.com/2100-1027-5089448.html>

In an abrupt reversal, SunnComm Technologies said Friday that it would not sue a Princeton University graduate student who had published a paper that describes how to bypass CD copy protection technology simply by pressing the Shift key. SunnComm had angrily assailed Princeton doctoral student John "Alex" Halderman just a day before, claiming that his academic paper was "at best, duplicitous and, at worst, a felony." The company had pledged to file a civil suit against Halderman under the Digital Millennium Copyright Act (DMCA) and lobby federal prosecutors to indict him on criminal charges.

Archived at <http://www.politechbot.com/>

Moderated by Declan McCullagh (<http://www.mccullagh.org/>)

⚡ Microsoft to fix Windows - again

<"Gene Lambson" <genengail@earthlink.net>>

Thu, 9 Oct 2003 16:19:50 -0500

According to NewScientist

<http://www.newscientist.com/news/news.jsp?id=3Dns99994258>

Microsoft is making some changes to "fix" security problems with Windows - I

quote: "The update will make a program more likely to crash than let a

hacker in, Oaken says."

How nice. If you can't fix it make sure it breaks. Good thing MS

doesn't give advice to the airline industry.

⚡ Winning the security trifecta

<Jeremy Epstein <jeremy.epstein@webmethods.com>>

Fri, 10 Oct 2003 09:24:17 -0400

Reported in all the media... "The U.S. Securities and Exchange Commission

has filed civil charges against a Pennsylvania man for computer hacking and

identity theft in a scheme last July to dump worthless options for Cisco

Systems Inc. stock" (Computerworld). The story I heard on NPR is that he

sold "puts", and when they were about to close out and lose \$37,000, he

decided to take action. So he created a web site with a Trojan keyboard

logger, and enticed investors to visit his site with the promise

of stock charts. Those who bit (and downloaded his Trojan) had their passwords & account numbers stolen. He then logged into one of the stolen accounts, and transferred his (negative value) position to the victim.

Result: he's been indicted for securities fraud, hacking, and identity theft... the first time (according to NPR) that all three have been brought together... the "security trifecta".

The "moral" of the story given on NPR was that you should always check your statements, so you catch unexpected transactions. Seems to me that the moral of the story is that managing your finances, or anything else sensitive, using the Internet is inherently RISKY. Customers are being told that if they use SSL, everything is safe. But as all of us know, all SSL provides is a protected pipe, which can be used as effectively for attacks as legitimate transactions.

The RISKS, as we say, are obvious. But to tie it to Mercuri's comments on California voting in [RISKS 22.94](#) ... anyone who alleges that there's no practical way to subvert Internet voting should take a look at this case, assuming it's as claimed. It's not hard to imagine an over-enthusiastic campaign worker enticing voters to download a Trojan that causes votes to go the "right" way... especially in an election with 135 candidates where stranger things are happening every day.

Something's fishy with Diebold in California

<zowie@euterpe.boulder.swri.edu (Craig DeForest)>

Fri, 10 Oct 2003 09:19:56 -0600

Mark Crispin Miller asserted, on the basis of a statistical analysis of California counties and vote distribution in the recent gubernatorial circus, that votes appear to have been "skimmed" from front-running contenders and redistributed to definite non-contenders in counties that use Diebold voting machines.

<http://www.markcrispinmiller.blogspot.com/>

Out of curiosity, I visited the California election-return website

<http://vote2003.ss.ca.gov>Returns/gov/00.htm#cty>

and did a cursory analysis myself. It appears that the sum of all the votes for the sixth-runner through the bottom is not enough to change the outcome, even if they were all assigned to Bustamante (the second-place candidate): Schwarzenegger won by 1.3E6 votes, while all candidates below the top five only garnered 2.2e5 votes.

Nevertheless, I agree with Mark that the per-county statistics look very fishy: many of the minor candidates received a much higher percentage of the vote in those counties with Diebold machines, and the difference is strongly significant.

✶ Data transfer Excel-COBOL loses voter data

<"Patrick O'Beirne" <mail2@sysmod.com>>

Fri, 10 Oct 2003 09:50:58 +0100

<http://www.ddtonline.com/articles/2003/10/08/news/news2.txt>

Officials begin affidavit count, By Amy Redwine / Delta Democrat Times

More than 1,600 affidavit ballots remain to be counted from Monday's

Democratic primary, Greenville election officials said this morning, when

officials began counting the affidavits in City Council chambers.

City Attorney Andy Alexander explained why there were so many affidavits.

He said the city had to go through a three-step process for elections: The

first part was getting the voting books from the county and checking them.

After that step was completed, the names were added to an Excel spreadsheet

in the city's computer. "The information from Excel had to be entered into

another database, COBOL. Apparently what happened is that when the rolls

were printed, all the information did not get transferred," Alexander said.

"Entire neighborhoods were left off of the voter rolls."

Patrick O'Beirne, Systems Modelling Ltd., Villa Alba, Tara Hill, Gorey,

Co. Wexford, Ireland <http://www.sysmod.com> Tel. +353 55 22294

✶ The shape of elections to come in England

<"C.Cartledge" <C.Cartledge@sheffield.ac.uk>>

Fri, 10 Oct 2003 16:02:47 +0100

Given the comments on the use of technology in US elections, readers may be interested in the approach being recommended by the body responsible for overseeing elections in England. Hand counting of ballot papers is the norm in England and is implicitly retained in the information referenced.

There is no mention of dedicated voting equipment, but there are innovations such as:

The roll-out of all-postal elections (The English are careful with their use of new technology - it is 163 years since the "penny post" was established here.)

The use of watermarked ballot papers to replace the stamped official mark as proof of authenticity;

Barcodes to replace serial numbers on ballot papers

All-postal voting should be made the norm at all local elections throughout Great Britain, says The Electoral Commission in its evaluation of voting trials at the May 2003 local elections in England[1]. In its independent report, The shape of elections to come, the Commission also concludes that further piloting of electronic voting is essential before setting a date for an e-enabled general election. ... 31 Jul 2003

See full press release at:

<http://www.electoralcommission.gov.uk/media-centre/newsreleasereviews.cfm/news/214>

The English are careful with their use of new technology. It is

after all
just 164 years since the "penny post" was established here.

✶ Risks of living in New Mexico

<"Hartfield, Kent" <kent.hartfield@lmco.com>>
Wed, 08 Oct 2003 07:31:45 -0500

[The main risk of living in New Mexico is trying to make a phone purchase from another state and being told they don't ship to foreign countries, but that's another matter.]

Risks of Living in New Mexico?

This happened last week to a friend of mine in Taos, New Mexico.

Event one. Friend gets purse stolen at school she teaches at. Doesn't report it for an hour thinking it was misplaced.

Event two. She finally reports purse stolen. Notifies one of two credit card companies about theft, can't notify the second card company because she can't remember who issued it (had the card for years but never used it).

Event three. Wal-Mart calls and said the "unknown card" was used at their store by a former employee. Wants to know if she was authorized to do this. Wal-Mart brought up to speed on events of the day.

Event four. Now card issuer is known since Wal-Mart revealed it. Friend calls and cancels card. Told many purchases are made on card around town.

Card cancelled.

Event five. Find out that not only did cashier at Wal-Mart know the person using stolen card, cashier also knew the real owner of the card, but didn't make the connection since the card listed the first name but she knew the owner only by her middle nickname. Small but slightly disconnected world.

Event six. Go to Department of Motor Vehicles to get new driver's license. Need Social Security card as identification, but that was stolen too. Finally DMV acquiesces to accept passport. Reports that person can't get new driver's license since didn't have valid driver's license to start with since not renewed two years ago.

Event seven. Disagree with DMV clerk. Clearly remembered renewing license since did it same day husband renewed his. Call husband to get day of renewal off of his license. Clerk reports husband doesn't have valid renewed license either even though husband comes to office to display actual license. Physical evidence does not take precedence over computer records.

Event eight. Police not yet arresting "perp" for unauthorized use of credit card even though recorded on video and ID'ed by clerk. Police inform friend and husband they are lucky they found out their drivers licenses were invalid since they would have been arrested if stopped for any routine traffic violation.

OK, so it took to Event Seven to get a computer risk out of

this. Still,
wasn't this a fun story?

[They don't yet know why their licenses were not in the
system, even
though they were issued physical licenses. KH]

Kent Hartfield, Lockheed Martin Missiles and Fire Control

[Re: Unencrypted credit-card submission forms \(Silverberg, R-22.92\)](#)

<"Jeffrey W. Baker" <jwbaker@acm.org>>

Thu, 09 Oct 2003 20:04:02 -0700

The "Snake Oil Ltd." certificate is indeed a testing certificate. Specifically, it is the self-signed certificate generated by the installation procedure of Apache-SSL. The presence of this certificate does not make your SSL connections less secure: they will still be encrypted and therefore difficult to intercept or corrupt.

What the web server at "Linux Web Toast" is saying is "Our name is company XYZ, just take our word for it." Your software (the browser) is bringing this to your attention because it is not configured to just take anybody's word for anything. A normal secure web server would say something like "Our name is company XYZ according to VeriSign, Inc, and you can take their word for it." Your web browser is probably configured to automatically trust VeriSign, Inc.

I hope you see the risks here. Why would you trust VeriSign?

They are one of the least trustworthy organizations I can think of. See "VeriSign responds with arrogance to Site Finder critics" [<http://www.siliconvalley.com/mld/siliconvalley/6960632.htm>] and "VeriSign settles FTC complaint" [<http://news.com.com/2100-1025-5081941.html>].

Do you realize, when you are using your web browser, that you implicitly trust this distant corporation? Does the average user of the Internet have any understanding of certificates and trust graphs? Is there any particular reason to trust VeriSign more than you trust, say, me, or your barber, or the guy who lives around the corner?

A further risk is that VeriSign operates a toll gate to the Internet. As the previous correspondent has ably demonstrated, you must pay VeriSign to sign your SSL certificate or you will lose customers. In this way VeriSign has electronic commerce cornered.

The final risk is that VeriSign acts as a single point of failure in the trust system. Anyone who compromises VeriSign's root private keys will be able to issue legitimate-sounding certificates claiming to be anyone. VeriSign has previously been tricked into issuing certificates in the name of Microsoft Corp. and other entities [[RISKS-21.29](#),30,32]

PS: I checked the certificate of linuxwebhost.com, and it appears to be signed by Equifax, not self-signed.

Re: Hidden risks: location dependence ([RISKS-22.85](#))

<msb@vex.net (Mark Brader)>

Fri, 10 Oct 2003 01:26:56 -0400 (EDT)

Another surprising location-dependency led to a key discovery in nuclear physics, according to Richard Rhodes in "The Making of the Atomic Bomb" (1986, Simon & Schuster, ISBN 0-671-44133-7).

In 1934, physicists Edoardo Amaldi and Emilio Segre were exposing samples of various elements to streams of neutrons: they hoped for a reaction where the neutrons would be captured, creating a new isotope that would be revealed by its radioactivity. This worked, but they found that the results varied greatly according to **where in the lab** they did the experiment.

This was in Italy, where marble was cheap enough that some of the lab tables were made of it. And as it turned out, that was the difference: more neutrons were captured when the experiment was done on a wooden table than a marble one.

It was Enrico Fermi who figured it out: neutrons were captured more easily if they were moving slower. Wood, unlike marble, contains a substantial proportion of hydrogen atoms, which are the right size to slow some of the neutrons and deflect them back. And in this way the concept of a moderator for nuclear reactions was discovered.

(I suppose that in this particular case, some people may feel that the Risk was that nuclear reactions **would** be discovered!)

[Old item. Catching up, thanks to Mark's prompt. PGN]

⚡ Re: Identity Denial really exists (Clark, [RISKS-22.93](#))

<Paul Wallich <pw@panix.com>>

Wed, 08 Oct 2003 09:49:01 -0400

Depending on what's meant by "cancel" this doesn't seem too uncommon or unlikely. Death certificates in many US states, for example, can be forged with relatively basic tools, and some institutions don't require even that level of proof. And the corpse will find out only if they try to use some service that depends on being officially alive. (Some years back, I was surprised to receive condolences from a pension-fund officer on the ostensible demise of a sibling -- who was similarly surprised to hear of the event.)

⚡ Re: Too much spam filtering

<John Bechtel>

Wed, 8 Oct 2003 10:07:07 +0100

I read with interest the item in [RISKS-22.92](#) about spam filtering for good e-mail, and note as well the comment about not trusting your ISP. I have recently had to change my ISP from AXX (name changed) because of

their aggressive spam filtering policy. AXX advertise that they aggressively filter spam, and equally go after spammers. I applaud the attitude. I cannot applaud their mechanism.

After too many games of "Did you get my e-mail?" ... "What e-mail?" leading to missed appointments and what-have-you I was told that 1) AXX was spam filtering my e-mail even though I had set my account not to filter anything, 2) I would not be allowed to see or change the policies used to decide what was spam and what wasn't, 3) It was not possible for me to see what was being "filtered" in order to rescue it, and 4) Filtering could not be turned off. After I gave them a list of addresses that I knew were being blocked I was told that AXX had detected spam from their ISPs... not my people specifically, just the ISP. I was told it was best for me to contact those people's ISPs to ask the ISPs to stop allowing spam. Only then would AXX stop deleting my e-mail. BTW, I don't consider that AXX was filtering my e-mail... they were deleting it, at random, without notice.

They produced some discussion about possibly being able to selectively allow specific addresses, in the concept of allowing known addresses through, but were not sure it would work, and of course that would not solve the problem of e-mails from third parties that I do want being filtered never to be seen again.

I believe some new versions of AXX can allow users more control since

then, but I was not told about that at the time (1 month ago),
nor am I
sure now, nor do I care.

John Bechtel, 1 Farnham Road, Guildford, Surrey, UK, GU2 4RG

✂ Observed sudden 1400-fold increase in W32/Swen infected e-mails

<Jon Seymour <jon.seymour@acm.org>>

Thu, 09 Oct 2003 04:10:21 +1000

I'd like to draw attention to a phenomenon associated with the
W32/Swen
worm with which I have just painfully become acquainted.

At 10pm, October 7 Sydney time (12:pm October 7 GMT), I noticed
a sudden
increase in the number of W32/Swen-infected e-mails that my spam
filter was
detecting.

To put the increase in perspective. Between September 23 and
October 7, I
had received 12 e-mails infected with W32/Swen. With each e-mail
weighing in
at roughly 145kB that's around 6kB per hour over 298 hours.
Irritating, but
tolerable. Starting at 10pm October 7, I started receiving one
of these
145kB e-mails every 6 minutes.

That's a 1400-fold increase in the rate of W32/SWEN infected e-
mails hitting
my inbox.

And as I write this, over 28 hours later -- it still hasn't
stopped. I am

still receiving infected e-mails -- from a wide variety of different hosts

-- at the roughly same rate as when the deluge started at 12:00 GMT on 7

Oct. That's an inbound rate of 38MB in one day. If it keeps going at this

rate, my mail box will receive about 1GB of this stuff each month.

Some points of note:

- * The e-mails appear to originate from random ISP accounts around the world.

- * There is no reason to believe that my e-mail address was harvested from the local address books of these machines -- suggesting that these zombies are acquiring their address lists from some external agency.

- * Each account is responsible for a small number (usually < 3, always less than 6) e-mails.

- * From my perspective, this is not an exponential growth characteristic - more of a step - suggesting that these infected hosts were "switched on" at 12:00 GMT, perhaps because my e-mail address was added to some pool of addresses at that time.

So, the lesson here is: even if you keep your virus software up to date, discard all suspicious e-mail, don't use peer-to-peer software, install a personal firewall, yada, yada, yada you can still fall victim to a worm created by a suitably deranged mind.

[Added note, Fri, 10 Oct 2003 08:38:59 +1000:]

I understand what the trigger for the deluge was now. Unfortunately, I

hadn't read:

<http://www.f-secure.com/v-descs/swen.shtml>

If I had, I would have realised that a post to USENET would have this effect.

So, it would appear that, if the consequence of posting to USENET is to provision oneself with a 38MB/day stream of virus-laden spam, it would then seem that USENET is now effectively, finally, dead.

Re: Difficulties with Census Bureau income data (Mannes, RISKS 22.93)

<Tony Lima <TonyLima2@att.net>>

Thu, 09 Oct 2003 15:15:53 -0700

[I took the liberty of asking my colleague Dr. Nan Maxwell about this issue. Her reply is below (forwarded with her permission, naturally).

Dr. Maxwell is Director of the Human Investment Research and Education

Center at California State University, Hayward. She is also Professor of

Economics and a respected researcher into the relationship between

demographics and economics. Tony Lima]

Thu, 09 Oct 2003 08:54:02 -0700, "Nan Maxwell"

<nmaxwell@csuhayward.edu>

The census has always capped income figures (as the article notes) for reasons of confidentiality.--if there are 26 people in the us making over \$1 million and you know their gender, race, place of residence,

industry,
occupation, etc. you can pretty much guess who they are. When I first started in this business the cap was \$100,000!!! The cap has always been the source of discussion like the one below, but confidentiality always wins. (And I guess I believe it should). The real question (in my mind) is...has the cap become more constraining over time?

Nan L. Maxwell, Co-Chair and Professor of Economics and Executive Director,
HIRE Center, Cal State University, Hayward College of Business and Economics
25800 Carlos Bee Blvd., Hayward, CA 94542 510.885.3191

✦ **Re: Getting over that fishbowl feeling (Smith, [R-22.94](#))**

<[Identity withheld by request]>
10 Oct 2003 09:02:18 -0400

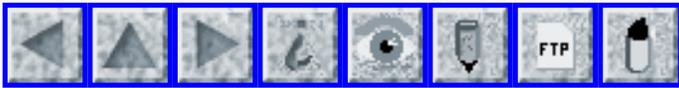
> A piece of evidence he presented to support this was a set of estimates of
> the street value of ID information: \$1 for a valid card number, \$5-10 for
> one with personal info to back it up (name, addr, etc), and \$10-15 if it
> includes the CVV2 number from the back ...

The numbers are high, by about three orders of magnitude. The normal way to quote prices of stolen credit card numbers is for a thousand. Prices such as \$10 to \$60 per 1000 numbers are not unusual (the price depends on the presence of billing information and CVV2 code, but mostly on the pseudonymous reputation of the seller). It is easy to purchase

the numbers
on the net anonymously (but credit card payment will not be
accepted).



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 22: Issue 96

Saturday 18 October 2003

Contents

- [Building cleared after computers blow](#)
[Graham Smith](#)
- [Car navigation system led tourist into supermarket](#)
[Michael Borek](#)
- [The Joy of Good Design](#)
[NewsScan](#)
- [Top 10 data disasters](#)
[NewsScan](#)
- [Billboard slip adds to humiliation for Chicago Cubs](#)
[Bill Higgins](#)
- [The Future of Surveillance](#)
[Bruce Schneier](#)
- [Hacker charged with securities fraud](#)
[NewsScan](#)
- [More on the California recall election](#)
[Rebecca Mercuri](#)
- [Re: Something Fishy about Diebold](#)
[Doug Sojourner](#)
- [Re: Continental taking back mistaken transactions](#)
[Phil Reed](#)
- [Re: Satellite photo of Eastern North America during blackout](#)
[Mark Brader](#)
- [Deadlock in Licensing Agreement, Dell Dumped](#)

Mark Brader

● 'Lover Spy' software

Geoffrey Brent

● Re: Unencrypted credit-card submission forms

Bill McGonigle

● Re: Benjamin Franklin

Jay R. Ashworth

● Re: W32/Swen: And I thought I had it bad...

Jon Seymour

● Info on RISKS (comp.risks)

✂ Building cleared after computers blow

<gks@cix.compulink.co.uk (Kildwick Smith Ltd)>

Thu, 16 Oct 2003 11:32 +0100 (BST)

I bet your company's business risk list doesn't include computers blowing up! <grin>

submitted by Graham Smith from

[http://www.thisislincolnshire.co.uk/displayNode.jsp___?
nodeId=57711&command=displayContent&sourceNode=57238&contentPK=7422650](http://www.thisislincolnshire.co.uk/displayNode.jsp___?nodeId=57711&command=displayContent&sourceNode=57238&contentPK=7422650)

Building cleared after computers blow
Lincolnshire Echo, 16 Oct 2003

An office building was evacuated on 15 Oct 2003 after 30 computers exploded. Around 400 members of staff at HBS Business Services, in Brayford Wharf North, Lincoln, left the building just after 12.15pm. Computers in one block of the building had blown up, producing smoke and setting off the fire alarms. Workers had to wait for more than 90 minutes before they could return to their desks. The cause was an electrical. All the computers have

to be replaced.

⚡ Car navigation system led tourist into supermarket

<mikkeles@netscape.net (Michael Borek)>

Thu, 16 Oct 2003 12:15:46 -0400

A US tourist's trip through Bavaria ended with an unexpected visit to a supermarket when his car's navigation system led him straight through the store's doors. He depended entirely on the navigation system and did not notice approaching the supermarket until entering it. [Source: Ananova News]

http://www.ananova.com/news/story/sm_828633.html?menu=news.quirkies

There are details neither on the navigation system in use nor the reason why it "thought" there was a carriageway there. I could see the cause being either inaccurate maps (data) or a failure in the resolution of the code (assuming that the algorithms work, of course!). In any case, the inattention (or misplaced attention) of the driver, who had been celebrating, is a significant factor.

⚡ The Joy of Good Design

<"NewsScan" <newsscan@newsscan.com>>

Tue, 14 Oct 2003 09:05:00 -0700

Design guru Don Norman says the way a device looks, feels and gives pleasure is just as important as how it works, and that good design can make up for some -- though not all -- shortcomings. "How attractive something is

will mean people will overlook some of the bad functionality, but not completely." His new book, "Emotional Design: Why We Love (or Hate) Everyday Things," -- due out in 2004 -- focuses on the way design works at different levels of brain perception. "The visceral level is the low biological level and that's where beauty comes in and appearances matter. On the surface something looks attractive and feels good. That is very important and that makes the brain function differently," says Norman. The behavioral level, which controls muscles, perception and language, perceives an object's usability and how it feels. But Norman says the most important aspect of design is its ability to invoke the deeper level of reflection, the level that dictates how we feel about things. "That is where having a good brand name matters. Having a good brand name has to be earned because they stand for trust." Good emotional design must incorporate all three levels, and Norman cites Apple and Sony as two companies that have managed to do that well. [BBC News 14 Oct 2003; NewsScan Daily, 14 October 2003]
<http://news.bbc.co.uk/1/hi/technology/3175506.stm>

✶ Top 10 data disasters

<"NewsScan" <newsscan@newsscan.com>>
Thu, 16 Oct 2003 09:09:05 -0700

Although machine failure is at fault for the majority of lost data disasters, humans are increasingly culpable as well, according to recovery experts at Kroll Ontrack. "Despite being the easiest problem to prevent, we are seeing more cases where human error is to blame. Interestingly,

we see a 15 to 20% increase in calls to recover lost data on Mondays. This could be a result of the rush to complete work and leave early for the weekend on Friday afternoons, as well as a lack of staff concentration on Monday mornings," says a Kroll spokesman. The Top 10 list of unusual data loss stories includes laptops being shot or thrown against the wall in a fit of e-rage; laptops suffering spills of red wine or latte because users were "drinking on the job," laptops falling off mopeds or car roofs, then being crushed by oncoming traffic; and PCs being thrown out a window or into a river to destroy evidence of theft or fraud. Our favorite? The laptop that slipped into the bathtub with its owner while he was working on accounts. Amazingly, Kroll Ontrack says in all these cases, it was able to rescue and restore computer files. [BBC News 16 Oct 2003; NewsScan Daily, 16 Oct 2003]

<http://news.bbc.co.uk/1/hi/technology/3193366.stm>

🔥 Billboard slip adds to humiliation for Chicago Cubs

<Bill Higgins <higgins@fnal.gov>>

Wed, 15 Oct 2003 11:20:04 -0500

Last night's baseball game was a difficult and disappointing one for the Chicago Cubs. For most of the game, they were ahead of the Florida Marlins in the struggle for the National League championship, entering the eighth inning with a score of 3-0. A fourth victory in the present series of playoff games would send them to the World Series-- which the Cubs have not reached since 1945-- so excitement was high.

During the eighth inning, a Cubs fan at the edge of the stands reached out and deflected an incoming ball, causing a player to miss catching it. Even worse, the Marlins began a fantastic rally that ended the eighth inning, and ultimately the ballgame, with a score of 3-8.

So, as I write this, the playoff series is 3-3, and tonight's game will decide the contest.

This morning I heard WXRT radio report that "somebody at Budweiser hit SEND instead of DELETE," causing an animated highway billboard to spell out "CONGRATULATIONS 2003 NATIONAL LEAGUE CHAMPION CHICAGO CUBS."

Obviously Budweiser's advertising people had the message ready for the contingency of a Cubs victory.

You don't suppose that the same fumble-fingered guy who knocked the ball away from the Cubs' outfielder works at Budweiser as a billboard operator?
Nah.

I hope that the appearance of the mistaken congratulations doesn't jinx the Cubs, and that Budweiser will be able to re-use the message tomorrow.

Bill Higgins Fermi National Accelerator Laboratory higgins@fnal.gov

[Unfortunately for the Cubs, that did not work out. But it was a great year for them anyway, and we are once again reminded that baseball is a game of inches. Same thing for the Red Sox (and Giants and Athletics).
Wait Till Next Year is always the operative slogan for all but the eventual winner. PGN]

<Bruce Schneier <schneier@counterpane.com>>

Tue, 14 Oct 2003 22:58:28 -0500

[From CRYPTO-GRAM, October 15, 2003]

At a gas station in Coquitlam, British Columbia, two employees installed a camera in the ceiling in front of an ATM machine. They recorded thousands of people as they typed in their PIN numbers. Combined with a false front on the ATM that recorded account numbers from the cards, the pair was able to steal millions before they were caught.

In at least 14 Kinko's copy shops in New York City, Juju Jiang installed keystroke loggers on the rentable computers. For over a year he eavesdropped on people, capturing more than 450 user names and passwords, and using them to access and open bank accounts online.

A lot has been written about the dangers of increased government surveillance, but we also need to be aware of the potential for more pedestrian forms of surveillance. A combination of forces -- the miniaturization of surveillance technologies, the falling price of digital storage, the increased power of computer programs to sort through all of this data -- means that surveillance abilities that used to be limited to governments are now, or soon will be, in the hands of everyone.

Some uses of surveillance are benign. Fine restaurants sometimes have cameras in their dining rooms so the chef can watch diners as they eat their creations. Telephone help desks sometimes record customer conversations in order to help train their employees.

Other uses are less benign. Some employers monitor the computer use of their employees, including use of company machines on personal time.

A company is selling an e-mail greeting card that surreptitiously installs spyware on the recipient's computer. Some libraries keep records of what books people check out, and Amazon keeps records of what books people browse on their website.

And, as we've seen, some uses are criminal.

This trend will continue in the years ahead, because technology will continue to improve. Cameras will become even smaller and more inconspicuous. Imaging technology will be able to pick up even smaller

details, and will be increasingly able to "see" through walls and other barriers. And computers will be able to process this information better.

Today, cameras are just mindlessly watching and recording, but eventually

sensors will be able to identify people. Photo IDs are just temporary;

eventually no one will have to ask you for an ID because they'll already

know who you are. Walk into a store, and you'll be identified. Sit down at

a computer, and you'll be identified. I don't know if the technology will

be face recognition, DNA sniffing, or something else entirely. I don't know

if this future is ten or twenty years out -- but eventually it will work

often enough and be cheap enough for mass-market use. (Remember, in marketing, even a technology with a high error rate can be good enough.)

The upshot of this is that you should consider the possibility, albeit remote, that you are being observed whenever you're out in public.

Assume that all public Internet terminals are being eavesdropped on; either don't

use them or don't care. Assume that cameras are watching and recording you

as you walk down the street. (In some cities, they probably are.)

Assume that surveillance technologies that were science fiction ten years

ago are
now mass-market.

This loss of privacy is an important change to society. It means that we will leave an even wider audit trail through our lives than we do now. And it's not only a matter of making sure this audit trail is accessed only by "legitimate" parties: an employer, the government, etc. Once data is collected, it can be compiled, cross-indexed, and sold; it can be used for all sorts of purposes. (In the U.S., data about you is not owned by you. It is owned by the person or company that collected it.) It can be accessed both legitimately and illegitimately. And it can persist for your entire life. David Brin got a lot of things wrong in his book *The Transparent Society*. But this part he got right.

Kinko's story:

<<http://www.computercops.us/article2568.html>>

<<http://www.securityfocus.com/news/6447>>

ATM fraud story:

<<http://www.globetechnology.com/servlet/story/RTGAM.20030812.gtatmm0812/>

<[BNStory/Technology](http://www.globetechnology.com/servlet/story/RTGAM.20030812.gtatmm0812/)>

<<http://canada.com/search/story.aspx?id=f07cac50-62c7-46d8-892a-b66dfa2f1d88>

<[1d88](http://canada.com/search/story.aspx?id=f07cac50-62c7-46d8-892a-b66dfa2f1d88)>

Net spying:

<<http://www.nytimes.com/2003/10/10/technology/10SPY.html>>

<http://news.com.com/2100-1029_3-5083874.html>

Hacker charged with securities fraud

<"NewsScan" <newsscan@newsscan.com>>

Fri, 10 Oct 2003 08:42:05 -0700

A 19-year-old student at Drexel University in Pennsylvania is being charged by the Securities & Exchange Commission (SEC) of fraud and identity theft for hacking into someone's investment account and making a complex and illegal trade. The student is accused of using a program called the Beast to monitor every keystroke typed on the target machine, and by doing so was able to obtain the log-in and password for the investor's online brokerage account with TD Waterhouse. [**The New York Times**, 10 Oct 2003; NewsScan Daily, 10 October 2003]
<http://partners.nytimes.com/2003/10/10/business/10HACK.html>

🚩 More on the California recall election

<"Rebecca Mercuri" <notable@mindspring.com>>
Mon, 13 Oct 2003 17:31:08 -0400

The following Web site contains some useful information pertaining to the California recall election and the resulting residual vote totals:
<http://www.votewatch2003.com/forum/showthread.php?p=983#post983>

It provides polling data on questions that specifically asked "did you have problems using the voting machines" (yes 2%) and also "did you not vote for question xyz". The latter result was off by 2% from the semi-official vote totals indicating either that (a) the 2% of people that had problems using the machine weren't able to cast their vote properly, or (b) there are 2% of the votes being lost by the machines, or (c) the polling data is 2% low. (I

am trying to find out how close they were on the totals for "what did you vote for" to see if (c) is really the case rather than (a) or (b).) Also, please note the caveat that everything is unofficial until the SoS posts the certified results, which will not occur until mid-November.

✶ Re: Something Fishy about Diebold

<Doug Sojourner <dsojourner@matrixsemi.com>>

Thu, 16 Oct 2003 13:28:56 -0700

Actually, all these numbers are so small that I don't think there is much here. The most significant case (Palmier) has the Diebold counties giving 3700 votes out of a total (in those counties) of 1300000, and outside Diebold counties 1500 votes out of a total of 6500000. I believe this means that in Diebold counties Palmier got 0.19% of the vote, with a sigma of 0.086%, and outside of Diebold counties 0.023% of the vote with sigma of 0.039%. With a null hypothesis that these both correspond to the same underlying probability of being voted for, I believe that the likelihood of this (the null hypothesis) happening is greater than $f(0.19/0.86)*f(0)$, which is about 3%. That leaves this on the edge of statistical significance. The most dramatic case (Kunzman) actually has more than 8% chance that the null hypothesis is true. I didn't compute any others, but I doubt they could do better than Kunzman.

So even though I distrust Diebold, I'm not sure this is strong evidence of tampering.

[On the other hand there are various alternative scenarios... With all of the different ballot faces, the mapping of vote positions to vote tallies is always a potential problem, either accidentally or intentionally (and in the latter case, not necessarily deterministic). Butterfly ballots add difficulties for the voters. If there are many more bad programmers than malicious ones, the election folks who insist that nothing can go wrong are seriously suspect. PGN]

✈️ Re: Continental taking back mistaken transactions ([RISKS-22.94](#))

<phil reed <phillipcreed@yahoo.com>>
Fri, 10 Oct 2003 06:24:29 -0700 (PDT)

Reading the tale of Continental Airlines taking back free miles reminded me of a tale of woe from a few years ago.

A former employer (now defunct) was implementing a direct-deposit function for their payroll. The actual payroll processing had been outsourced for some time to a large company that does this sort of thing routinely (name left out because they are still in business). As part of setting up the direct deposit, the payroll group collected bank account numbers and passed them along to the outsourcing company, who entered them in their various databases. Everything normal, nothing exceptional.

As part of the checking process that looked for routine data entry errors, the outsourcing company's strategy was to run a complete end-to-end sequence

that would perform an actual deposit of \$0.00 into everybody's account. This would cause all the invalid bank account numbers to show up on the normal error report, so they could be corrected before running an actual payroll and accidentally not paying somebody on payday.

You can probably guess what happened next: the test deposit was run, but with actual payroll amounts, not with a zero dollar deposit. The error was discovered after about an hour, and it took another couple of hours to prepare a "reverse deposit" transaction to get the money back out of the accounts. During that 3 hour window, a handful of people (almost all of them spouses of factory workers) discovered the extra money and withdrew it from their checking account. Some of them immediately spent it.

I don't know who it was that had to tell those workers that they had to return the money, but I cannot imagine that it was a very pleasant job.

✶ Re: Satellite photo of Eastern North America during blackout ([R-22.88](#))

<msb@vex.net (Mark Brader)>

Fri, 10 Oct 2003 01:28:51 -0400 (EDT)

[Originally submitted 29 Aug 2003, lost in the shuffle. Sorry. PGN]

In addition, if the UTC timestamps on the two photos are correct, then the labeling as "20 hours before" and "7 hours after", seen both in the images and their URLs, is wrong -- as is obvious because the two times are about 24

hours apart! The blackout actually at 4:10 pm EDT (give or take a couple of minutes, depending on location): that's 20:10 UTC, so the pictures are 19 hours before and 5 hours after. The first error looks like someone forgot about daylight saving time, but the second is harder to guess an explanation for.

> However, there is a surprising amount of light still on, ...

I don't see why John is surprised at this, since the article Andrew quoted says that "in the New York region .. nearly 20 percent of the available electricity remained on..." It seems natural that at the scale of a satellite photo we would not be able to tell which areas of the city were darkened and which were not.

(Toronto, as noted, is pretty much gone in the second photo -- and that's correct. During the blackout I was listening to local radio stations that invited people to phone in with information about their neighborhood, and there sure weren't any calls that said "we never lost power".)

🔥 Deadlock in Licensing Agreement, Dell Dumped

<msb@vex.net (Mark Brader)>

Fri, 10 Oct 2003 01:30:22 -0400 (EDT)

[Also originally submitted 29 Aug 2003]

Ian Goldberg writes at <<http://www.cypherpunks.ca/dell.html>> about his recent experience buying a Dell computer in Canada. In brief, the startup screen required him to declare that he had first read and then agreed

to the relevant license agreements -- but the agreements themselves were shrink-wrapped and could not be read without first agreeing to them.

Deadlock, and nobody he could reach at Dell even saw it as a problem.

✶'Lover Spy' software

<Geoffrey Brent <g.brent@student.unsw.edu.au>>

Tue, 14 Oct 2003 09:57:18 +1000

As reported in various news outlets recently, 'Lover Spy' offer a service for jealous lovers looking to spy on their partners:

"Using this very web site, you can very easily send Lover Spy as an e-greeting card. The e-card looks just like a normal e-greeting card sent via e-mail. When opened, it will display a graphic of your choice, whether it be romantic flowers, a funny e-joke, or kittens. But silently, this e-card will secretly install our award-winning spy software on their PC !
..."

The spyware then reports back to Lover Spy's customer with a record of websites visited, chat sessions logged, passwords captured, etc etc. Site

is currently down (hopefully for good), but can be viewed in Google's cache:

<http://tinyurl.com/qsyd> (full Google link at the end of this message, for those who don't like tinyurl).

There are several very obvious reasons why this is a Bad Thing (not to mention illegal), and I doubt anybody on RISKS needs to be told the risks

this poses to the unwitting recipient of the greeting card. However, at

least one message-board poster (see link below) has suggested a more subtle

angle: presumably this service also requires the customer to install

some
form of software on their own computer to receive the data collected
from
their unsuspecting partner.

What are the chances that the customer-end software is *also*
spyware? As
any con-man knows, the easiest way to hoodwink your mark is to let
him think
he's hoodwinking somebody else. And when the scheme they sign up for
is
illegal - as this one most certainly is - then they're much less
likely to
squeal when they find out who the real target is. You're already
giving
Lover Spy your credit card number just by signing up for your service
- and
captured bank account details etc. could be the icing on the cake.

http://george.hotelling.net/90percent/linkage/lover_spy.php
[http://www.google.com.au/search?q=cache:7JvdodIm7xoJ:www.gootle.us/
technology.
php+%2B%22lover+spy%22+%2Bgreeting&hl=en&ie=UTF-8](http://www.google.com.au/search?q=cache:7JvdodIm7xoJ:www.gootle.us/technology.php+%2B%22lover+spy%22+%2Bgreeting&hl=en&ie=UTF-8)

🔥 Re: Unencrypted credit-card submission forms

<Bill McGonigle <bill@zettabyte.net>>

Fri, 10 Oct 2003 11:48:42 -0400

One of the criticisms of the HTTPS/SSL/TLS protocol is that it
provides both
encryption and authentication without the option to forgo either. In
this
case, the host has used a default certificate name generated by,
probably,
the OpenSSL toolkit. Note, it's not a sample certificate, it's
randomly
generated at install time, so the user needn't fret a man-in-the-
middle
attack. So, in this case, you have encryption but not
authentication. If

you're confident of the host name and can somehow verify that a DNS spoof isn't being employed (known IP, DNSSEC), you're good to go. Of course, it's not reasonable for the general population to make this verification.

For the princely sum of up to \$900 per year per hostname, SSL vendors like Verisign will sign a certificate for you saying that you are who you claim to be. Your web browser will trust the certificate and not display a warning because, e.g. Verisign's certificate is built into your web browser.

The trouble is, the amount of verification many certificate vendors go through is minimal (some require only a faxed letter on company letterhead), you have to trust the signer, and your certificates can be stolen (only some browsers support certificate revocation). So, critics charge that all you have is a false sense of security, which can be a greater risk. Some people fail to buy a 'real' certificate for cost reasons and some for philosophical reasons. Most just go ahead and pony up the cash to make the warning go away for the users.

✉ **Re: Benjamin Franklin ([RISKS-22.93-94](#))**

<"Jay R. Ashworth" <jra@baylink.com>>
Mon, 13 Oct 2003 14:06:05 -0400

> Ben's original quote also gives the Patriot Act guys plenty of wiggle room,
> by using the phrases "essential liberty" and "temporary safety."
Who's to
> judge "essential" and "temporary"?

Franklin himself, I think. He wasn't providing interpretative wiggle room

there, IMHO, he was making *another* value judgment: that liberty *is* essential, and security often only temporary. Remember the environment *they* lived in... it was, likely, much closer to today's America than 3 years ago's America... and yet they did what they did.

Why can't *we* (, Mr Ashcroft)?

Jay R. Ashworth, Baylink, The Suncoast Freenet, Tampa Bay, Florida
<http://baylink.pitas.com> +1 727 647 1274 jra@baylink.com

✶ Re: W32/Swen: And I thought I had it bad...

<Jon Seymour <jon.seymour@acm.org>>
Fri, 17 Oct 2003 09:27:59 +1000

Admittedly I was quickly disavowed of that notion by a few private responses to my last RISKS post - mine was but a mild dose of W32/Swen

And then this, from
<http://www.theage.com.au/articles/2003/10/16/1065917549896.html>

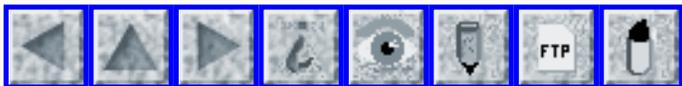
The Swen virus has been blamed for delaying e-mails to BigPond customers by up to several days. On 14 Oct 2003, BigPond reported its customers were receiving e-mails late due to a rapid rise in messages being sent and received through the network. E-mail messages had increased on average from about eight million to 13 million daily.

Spokeswoman Kerrina Lawrence today said the Swen virus was responsible for the sudden surge in traffic. "Telstra's technical staff has been working around the clock to establish additional network capacity to cater for the unexpected ... increase in e-mail traffic," she said in a statement. Ms

Lawrence said the additional capacity will help cater for the rise in messages. "Telstra understands that the virus/worm has been taking over customers' computers and using them to send large amounts of junk e-mails (spam)," Ms Lawrence said.

So, if only 1/2 of this 5 million per day increase is due to the e-mail containing the Swen worm (being generous and allowing for bounce messages), then Telstra is busily working to add an extra $2.5 * 1,000,000 * 145\text{kB} / (24 * 3600) * 8 \approx 32\text{Mbps}$ capacity to their e-mail network.

One presumes that they are also doing something about filtering so that all that extra capacity does not get eaten up by the worm, but then perhaps I presume too much.



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, [Peter G. Neumann](#), moderator

Volume 22: Issue 97

Thursday 23 October 2003

Contents

- [Computers may be bad for your health](#)
[NewsScan](#)
- [Recent London power outage](#)
[Peter Amey](#)
- [Justice Department e-censorship error](#)
[Kevin Poulsen via jones-gill](#)
- [RISKS Offshore: A tough lesson on medical privacy](#)
[David Lazarus via Scott Miller](#)
- ["Victoria's Secret Reaches a Data Privacy Settlement"](#)
[Drew Dean](#)
- [First DEWEY DEFEATS TRUMAN, and now YANKEES LOSE!](#)
[Mark Brader](#)
- [Discover cancels 60,000 accounts](#)
[Charlie Shub](#)
- [Nokia and mobile-phone battery explosions](#)
[Monty Solomon](#)
- [Teen rides Trojan Horse defense](#)
[Keith Rhodes](#)
- [Feds admit error in hacking conviction](#)
[Robert Lemos via ikanal](#)

- [Digital signatures: When will they learn?](#)
[Jeremy Epstein](#)
 - [Senate votes to can spam](#)
[NewsScan](#)
 - [Re: Difficulties with Census Bureau income data](#)
[Patrick J. Kobly](#)
 - [Re: Fun with stolen credit-card numbers](#)
[Dimitri Maziuk](#)
 - [Re: And I thought I had it bad...](#)
[Anthony W Youngman](#)
 - [Re: The Joy of Good Design](#)
[Debora Weber-Wulff](#)
 - [Info on RISKS \(comp.risks\)](#)
-

✂ Computers may be bad for your health

<"NewsScan" <newsscan@newsscan.com>>

Thu, 23 Oct 2003 09:39:21 -0700

Nine out of 10 computer users are stressed out by such regular occurrences as performance slowdown, spam overload and lost files, and the time wasted fixing problems just makes it worse, according to security firm Symantec. Anger management experts say computer stress must be alleviated before it affects productivity and human-to-human interactions. "If you are suffering from stress, the best thing to do is to breathe deeply, and remind yourself to keep your cool," says Mike Fisher, of the British Association of Anger Management. The top five stress triggers, according to Symantec, are: 1) Slow performance and system crashes; 2) Spam, scams and e-mail overload; 3)

Pop-up ads; 4) Viruses; and 5) Lost or deleted files. Men tend to freak out over viruses, spam and general information pollution, while crashing systems and sluggish performance really irk women. More than a third of both sexes will resort to extreme behavior during computer-related meltdown, including violence, swearing, showing and desperately hitting random keys. The good news is that 40% will actually try to fix the problem, often asking someone else for help. Symantec's Kevin Chapman suggests a few ways to reduce the potential for problems: "For example, don't download lots of large files and applications, and remove the clutter left behind by long periods on the Internet. To avoid spam, don't sign up for lots of mailing lists, and if you do receive spam-mail, never reply to it asking to be removed from the list as this will confirm your e-mail address." [Eds. Note: NewsScan never, ever shares your e-mail addresses with *anyone*, so we hope you'll stay on *our* list.] [BBC News 23 Oct 2003; NewsScan Daily, 23 Oct 2003]

<http://news.bbc.co.uk/go/pr/fr/-/1/hi/technology/3204719.stm>

Recent London power outage

<"Peter Amey" <peter.amey@praxis-cs.co.uk>>

Mon, 20 Oct 2003 09:49:36 +0100

The London power cut that followed shortly after the great New York blackout, was quickly blamed on an unforeseeable chain of events including

the fitting of an incorrect valued relay (widely reported as a "fuse"). It has now emerged that the root cause, the one which led to reliance on the incorrect relay and the power loss, was simple, old-fashioned poor maintenance.

The chain of events started when a sub-station transformer alarm sounded.

The problem at this transformer turns out to have been an oil leak which had been noticed and reported but not dealt with. A power company spokesman said on the BBC news that they couldn't necessarily take a transformer out of service as soon as a problem like this was found but, instead, had a system of managing the leak until it was convenient to correct the problem permanently. The problem in this case was that the leak wasn't managed (the request having passed into a planning centre described by one contributor as a "black hole"), the oil ran out, the alarm sounded, the transformer was switched out and the incorrect relay failed.

The risk I think is the rush to blame unforeseeable chains of events and freak failures rather than to admit to failures of basic preventive maintenance.

<http://news.bbc.co.uk/1/hi/england/london/3199594.stm>

<http://news.bbc.co.uk/1/hi/england/london/3199784.stm>

Peter Amey, Principal Consultant, Praxis Critical Systems, 20, Manvers St.

Bath, BA1 1PX UK +44 (0)1225 466991 www.praxis-cs.co.uk www.sparkada.com

Justice Department e-censorship error (Kevin Poulsen)

<<jonesgill@jones-gill.co.uk>>

Thu, 23 Oct 2003 06:19:33 -0000 (GMT)

Justice e-censorship gaffe sparks controversy

By Kevin Poulsen, SecurityFocus

Posted: 23/10/2003 at 09:37 GMT

Taken from www.theregister.co.uk

(<http://www.theregister.co.uk/content/55/33549.html>)

A government watchdog group Wednesday accused the Justice Department of improperly censoring portions of a key report on internal workplace diversity, after online activists successfully unmasked the blacked-out portions of an electronic copy of the document.

The 186-page report was released to the public under the Freedom of Information Act last week and posted to Justice Department's Web site in Adobe's "Portable Document File" (PDF) format. But the department blacked out vast portions of the document's text, citing an exemption to FOIA that permits agencies to keep internal policy deliberations private.

The text didn't stay concealed for long. On Tuesday a Web site called the Memory Hole, dedicated to preserving endangered documents, published a complete version of the report, with the opaque black rectangles that once covered half of it completely removed. Memory Hole publisher Russ Kick won't say how he unmasked it, but experimentation shows that the concealed text could be selected and copied using nothing more than Adobe's

free Acrobat Reader. Once copied, the text is easily pasted into another document and read.

It turns out the report began its life as a Microsoft Word document, and whoever was in charge of sanitizing it for public release did so by using Word's highlight tool, with the highlight color set to black, according to an analysis by Tim Sullivan, CEO of activePDF, a maker of server-side PDF tools. The simple and convenient technique would have been perfectly effective had the end product been a printed document, but it was all but useless for an electronic one. "Using Acrobat, I'm actually able to move the black boxes around," says Sullivan. "The text is still there."

In 2000, *The New York Times* made a similar error in publishing on its Web site a classified CIA file documenting American and British officials' engineering of the 1953 coup that overthrew Iran's elected leadership. Before releasing the document as a PDF file, the paper blacked out the names of Iranians who helped with the plot. But online intelligence archivist John Young published an unsanitized version of the report after discovering that the opaque black lines and boxes concealing the names could easily be removed.

Both cases demonstrate that what you see is not always what you get in electronic documents. Censors could have more effectively eliminated the text by deleting it, rather than painting it over. Additionally, commercial

software is available that's designed specifically to help government agencies redact PDF files for release under FOIA and the Privacy Act. Pennsylvania-based Appligent even sells its "Redax" Acrobat plug-in to the Justice Department. "The amazing thing is that there are different divisions in the Department of Justice that are using our software, so it's a little shocking that they would do this in Word," says company president Virginia Gavin.

Denuded of its censorious kludgework, the report -- produced last year by KPMG -- reveals much about the Justice Department's gender and ethnic diversity issues. But, significantly, it also shows that the department is overly aggressive in cutting documents for public release, according to the Federation of American Scientists (FAS). On Wednesday FAS wrote a letter to the Justice Department's Office of the Inspector General -- the DoJ's internal investigators -- urging a full investigation into officials' "unauthorized withholding of information."

"Too much information was withheld," says FAS's Steven Aftergood. "Information that was purely factual was censored as if it were deliberative... We want agencies to be able to discuss different policy options and to make recommendations outside of a charged political environment, and the deliberative exemption allows them to do that. But the exemption does not apply to factual material."

For example, a section of the text notes, "sexual harassment is not perceived by attorneys to be a problem in the Department, but racial

harassment is." That should never have been cut from the public version, says Aftergood. "That's something that ought to be made publicly available."

Much, if not most, of the scores of blacked out pages should have been released under law, Aftergood says. He credits the PDF blunder with exposing a systemic problem in the Justice Department's FOIA compliance, and he hopes an internal review will result in an overhaul of the system. A Justice Department spokesman declined to comment on the matter, and the almost-censored document disappeared from the department's Web site Wednesday afternoon. oops!

✶ RISKS Offshore: A tough lesson on medical privacy (David Lazarus)

<Scott Miller <SMiller@unimin.com>>

Thu, 23 Oct 2003 11:56:32 -0400

"Lazarus at large", David Lazarus, *San Francisco Chronicle*, 22 Oct 2003

"Your patient records are out in the open... so you better track that person and make him pay my dues."

A woman in Pakistan doing cut-rate clerical work for UCSF Medical Center threatened to post patients' confidential files on the Internet unless she was paid more money. To show she was serious, the woman sent UCSF an e-mail earlier this month with actual patients' records attached.

<http://www.sfgate.com/cgi-bin/article.cgi?file=/c/a/2003/10/22/MNGCO2FN8G1.DTL>

[Just one of the risks of outsourcing. PGN]

✶ "Victoria's Secret Reaches a Data Privacy Settlement"

<Drew Dean <ddean@csl.sri.com>>

Tue, 21 Oct 2003 14:37:41 -0700 (PDT)

That fabulous headline appeared in *The New York Times* online. Quick summary: Their Web site had a security problem where by anyone could check on the status of anyone else's order, although they could not get credit card information. Given the nature of the store, this is even more problematic than usual. Victoria's Secret paid a fine (\$50K) without admitting guilt. Interestingly enough, this happened under consumer protection laws, because Victoria's Secret violated their own privacy policy. Two good quotes -- the opening line: "There's private, and then there's private." and "'The core of it is, what do people expect will be kept secret? And of course when you're dealing with Victoria's Secret, you expect that a lot will be kept secret.'"

Full story:

<http://www.nytimes.com/2003/10/21/technology/21priv.html>

✶ First DEWEY DEFEATS TRUMAN, and now YANKEES LOSE!

<msb@vex.net (Mark Brader)>

Fri, 17 Oct 2003 16:57:06 -0400 (EDT)

The morning after the New York Yankees beat the Boston Red Sox to win the 2003 American League baseball pennant, early editions of the *New York Post* included an editorial bemoaning that the Yankees had lost. Apparently TWO versions of the editorial had been prepared, one for each eventuality, and the wrong one was published -- reportedly because someone hit "the wrong button." The AP item in the *NYTimes* began with ``The curse of the Bambino [Babe Ruth, erstwhile Red Sox pitcher, for non-baseball fans!] struck the *New York Post*, too.' ' ["NY Post Editorial Says Yankees Lost", 17 Oct 2003; PGN-ed]

<http://www.nytimes.com/aponline/national/AP-Post-Yankees-Editorial.html?ex=1067422908&ei=1&en=97f6f670437f48ef>

Discover cancels 60,000 accounts

<Charlie Shub <cdash@ludell.uccs.edu>>

Wed, 22 Oct 2003 13:07:19 -0600 (MDT)

On 15 Oct 2003, I received an e-mail from discover saying Your Discover(R) Card account is part of a group of accounts whose information may have been illegally obtained by unauthorized persons. As a protective measure, we will be issuing you a new account number. We

believe this proactive step is necessary to protect your account from potential fraud activity.

After a heated conversation with the people at the other end of their 800 number, they agreed to keep my particular card active through the weekend as I was leaving on a trip early the following morning. They also assured me that in the interval between when the account was turned off and the new cards arrived, they would be able to authorize individual purchases via a manual override process. That statement proved to be false.

charlie shub University of Colorado at Colorado Springs
cdash@cs.uccs.edu <http://cs.uccs.edu/~cdash> 1-719-262-3492

✶ Nokia and mobile-phone battery explosions

<Monty Solomon <monty@roscom.com>>
Fri, 17 Oct 2003 08:00:47 -0400

Nokia Recommends Using Only Original Batteries with Nokia Products; All Investigated Mobile Phone Battery Explosions Caused by Non-Original Batteries
- Oct 17, 2003 07:23 AM (BusinessWire)

Recently, in the Netherlands a battery used in a Nokia 7210 mobile phone exploded. An investigation by Nokia experts clearly proved that the battery involved in the incident was not a Nokia battery.

Over the past months, cases have been reported of non-original mobile-phone

batteries exploding, causing damage to both batteries and phones. In all the reported cases, the battery has been a non-original battery. Nokia offers its cooperation to authorities in taking legal measures available against those who sell and distribute poor quality non-original mobile phone enhancements compatible to Nokia products.

In general, the reported incidents are due to an internal short circuit. An internal short circuit can be caused by careless design, an uncontrolled production process or a combination of both. Original Nokia batteries and chargers are designed and manufactured adhering to stringent safety and quality measures. These include very strict requirements regarding the materials and insulation used inside the batteries as well as continuous production control and intensive product testing. ...

<http://finance.lycos.com/home/news/story.asp?story=36124379>

⚡ Teen rides Trojan Horse defense

<rhodesk@gao.gov>

Fri, 17 Oct 2003 09:28:31 -0700 (PDT)

A UK teen, accused of launching a DDoS attack, was acquitted as a jury apparently believed his explanation that a hacker had exploited his computer with a Trojan Horse. [Source: Munir Kotadia, zdnet]

http://zdnet.com.com/2100-1105-5092745.html?tag=sas_email

⚡ **Feds admit error in hacking conviction**

<notsp_ikinal@ieee.org>

Fri, 17 Oct 2003 06:35:26 -0700 (PDT)

Federal prosecutors asked an appeals court to reverse a computer-crime conviction that punished a California man for notifying a company's customers of a flaw in its e-mail service. Bret McDanel had already served his 16-month sentence, and is on supervised release with curtailed computer access. The original conviction resulted from McDanel having notified customers of Tornado Development (subsequently defunct) that their e-mail was susceptible to attack. An appeal was filed by Jennifer Granick in Stanford's Law School. [Source: Robert Lemos, zdnet, 16 Oct 2003; PGN-ed]

http://zdnet.com.com/2100-1105-5092697.html?tag=sas_email

⚡ **Digital signatures: When will they learn?**

<Jeremy Epstein <jeremy.epstein@webmethods.com>>

Thu, 23 Oct 2003 14:20:25 -0700

Microsoft has a deal with the US Postal Service for Office 2003 where USPS will store a permanent record of a document, so anyone can validate the document for the next seven years. The goal is "to sign and secure

documents in a way that is legally binding". The record (which is presumably a signed hash) includes "a unique time- and date-stamped record based on the file's exact content". Sounds good... an unbiased third party is part of what you need.

However, there are problems:

- * WYSMNBWYS: What You Sign May Not Be What You See. Small fonts, hidden data, bits & pieces of deleted stuff lying around, etc. 'nuff said, especially given the legacy of examples in RISKS.
- * Incompatibility: How often has Microsoft introduced a version of Office that was compatible with any other version? Never! So why should we believe you'll be able to verify one of these signed documents... especially for the next seven years? Or that it'll look like the document that was "signed"? C'mon!
- * What safeguards this repository against tampering? If I can modify the document and the repository's view of what was signed, I can change history.

<http://www.computerworld.com/securitytopics/security/story/0,10801,86300,00.html?nas=SEC2-86300>

Senate votes to can spam

<"NewsScan" <newsscan@newsscan.com>>
Thu, 23 Oct 2003 09:39:21 -0700

The U.S. Senate has unanimously approved the "Can Spam" bill, sponsored by Sens. Conrad Burns (R-Mont.) and Ron Wyden (D-Ore.), which would ban the sleaziest techniques used by spammers to spew out millions of junk e-mail messages each day. Under the provisions of the bill, senders of unsolicited e-mail would be prohibited from disguising their purpose by using a fake return address or misleading subject line, and would no longer be allowed to harvest e-mail addresses off the Web to bulk up their lists. In addition, junk e-mail would be required to include a legitimate "opt out" function that recipients could use to get off lists. A provision proposed by Sen. Charles Schumer (D-N.Y.) authorizes the Federal Trade Commission to establish a "do-not-spam" list, similar to the recently implemented "do-not-call" list that blocks telemarketing calls. "Kingpin spammers who send out e-mail by the millions are threatening to drown the Internet in a sea of trash, and the American people want it stopped," said Wyden, who urged foreign countries to adopt similar measures. [AP 23 Oct 2003;

NewsScan Daily, 23 Oct 2003]

<http://apnews.excite.com/article/2031023/D7UBQISG0.html>

★ Re: Difficulties with Census Bureau income data (Lima, [RISKS-22.95](#))

<"Patrick J. Kobly" <patrick@kobly.com>>

Tue, 14 Oct 2003 17:31:34 -0600

Tony Lima <TonyLima2@att.net> relayed comments from Dr. Nan Maxwell that:

> The census has always capped income figures (as the article notes) for
> reasons of confidentiality.--if there are 26 people in the us making
> over \$1 million and you know their gender, race, place of residence,
> industry, occupation, etc. you can pretty much guess who they are.

This is a red herring. There really is no (or minimal) privacy risk at the data-collection side of things. These privacy concerns (while very real) shouldn't be dealt with with this kind of gross clipping at collection-time, but rather with reasoned bucketing schemes at aggregation and reporting time.

Once the data is collected, the census bureau then can do bucketing based on the character of the data - there is plenty of academic work on this subject and market researchers have been doing this for years -- such that we don't report on buckets small enough to individually identify people. There are issues that arise, including methods to infer numbers in an intersection of two aggregation queries where just requesting the intersection yields unreportable (for privacy reasons) numbers, but these issues can be addressed with careful analysis.

Even if the data is reported in unaggregated form (ie. some complete individual surveys are shown), bucketing of answers can still

have an
anonymizing effect...

There are a number of ways of dealing with confidentiality
issues without
killing the quality of your data.

✶ Re: Fun with stolen credit-card numbers (Maziuk, [RISKS-22.94](#))

<Dimitri Maziuk <dmaziuk@bmr.b.wisc.edu>>

Fri, 10 Oct 2003 14:33:33 -0500

I received a few e-mail replies to my post and since I'm not
subscribed to
the list I don't know how many replies went there. Or how many
bounced
because you didn't check my Reply-To address before sending
(sorry, too much
spam). I think I should clarify a couple of points.

Simplified transaction I described comes from personal
experience. I worked
at a place that had an EFT server supplied by the bank (vendor
approved by
the bank, actually). It talked to the bank via leased line and
generally
worked like an ATM -- sans magnetic card reader.

I wrote the software that talked to EFT server so I know exactly
what
information my software supplied to it: card number and
transaction amount.

Different banks/clearing houses may have different rules, but
unless you
know exactly what the rules are in every particular case,
there's no reason
to assume a particular vendor makes use of anything other than

card number.

(Obviously, they need an address to ship the goods to, but that has nothing to do with credit card payment.)

My other point was that none of the other information can be used as 100% reliable fraud indicator. Even the signature: I could take my wife's credit card, put my signature on the slip, and -- (in theory) our bank should honour that transaction. Even though my signature doesn't match the one on the back of the card, it's still valid for our joint account.

Ergo, if the vendor decides to do fraud detection they have to deal with false positives. Vendor who makes the living from selling stuff has financial incentive to assume that the positive was, indeed, false.

The form you signed probably said (in a very small print) that it's your, not someone else's, responsibility to check your statement for transactions you didn't authorize. So the vendor doesn't have to bother with fraud detection at all. (Aside: we ended up building a database of "known offenders" and analysing the logs for usage patterns. And I spent more time on the phone to fraud agencies than I ever wanted to.)

So the system is insecure by design. As for secure alternatives (and that's what keeps coming up in RISKS): there are two ways to authenticate you (credit card user, airplane passenger, computer user). It's either something you know (PIN, password), or for something you have (fingerprint, barcode tattooed into your forearm, face on the photograph on your

driver's

license). For either way to work reliably, two conditions must be met:

1. Authentication token must be established beforehand using trusted channel. (cf. e-mailing passwords unencrypted. (It's not clear if encrypting them does that much good here, as there's no reason to believe joe@aol.com account really belongs to John A. Doe of 123 Beltway, Washington, DC, but still...)) (Do you want to have to travel to Amazon's head office with your driver's license, birth certificate, and two reliable witnesses to leave your thumbprint there before they let you buy anything?) (Do you want your fingerprints to be instantly available to (potentially) anyone who declares themselves "an on-line vendor"?)

2. Token must be transmitted via trusted channel during the transaction. (cf. Web sites that accept your credit card information via non-encrypted HTTP connection.) (With biometrics you have to also verify operation of the scanner device and make sure the finger, eye, or what have you is actually attached to a living body -- naturally attached, not surgically.)

Of course for a bad guy there isn't much difference between torturing you to learn your PIN and chopping off your thumb to take it to thumbprint reader. If they want it bad enough, they'll figure out how to defeat the system.

Given a choice between having \$1000 stolen and having my thumb chopped off, I think maybe existing system is not that bad after all.

✉ Re: And I thought I had it bad... ([RISKS-22.96](#))

<"Anthony W Youngman" <Anthony.Youngman@eca-international.com>>

Tue, 21 Oct 2003 10:30:32 +0100

Take a look at the guff about Demon's mail screwup ... (demon.co.uk, demon.net).

They upgraded their mail systems to cope with the ever-increasing tide of spam etc. Unfortunately, due to a config mistake, this made the problem worse (I'm guessing their SMTP kick for dial-ups got screwed).

As a result, they ended up backing up and deleting all pending mail on their servers, correcting the config blunder, and then feeding it all back in over the next few days.

I very nearly got badly stuffed -- I e-mailed some personal work home on the Monday to work on. As an exam assignment, it HAD to be delivered to Uni for marking by the Friday. The e-mail arrived home Friday evening -- past the deadline! Fortunately I didn't need it to be able to carry on working.

✉ Re: The Joy of Good Design (Don Norman in NewsScan, [RISKS-22.96](#))

<Debora Weber-Wulff <weberwu@fhtw-berlin.de>>

Sun, 19 Oct 2003 23:19:31 +0200

> Design guru Don Norman says the way a device looks, feels and gives
> pleasure is just as important as how it works, and that good design can
> make up for some -- though not all -- shortcomings. [...] Good emotional
> design must incorporate all three levels, and Norman cites Apple and Sony
> as two companies that have managed to do that well.
> <<http://news.bbc.co.uk/1/hi/technology/3175506.stm>>

Yes, but. It doesn't cover all shortcomings. At least in Europe, Sony has just as bad a "hotline service" as the rest of the lot. I'm planning on purchasing a new laptop, and I just realized that my Sony Camera wouldn't talk to my Sony laptop (and the service center couldn't help) and my Sony PDA has flaky battery problems (and the service center couldn't help) that seemed to be linked to the Sony Memory Stick (if I take it out, it is less flaky). So I asked myself: do I really want another Sony? Of course, they are beautiful. My answer: no. Since all of the service centers tested "D" or "F" on a school grading scale (4 or 5 on the German scale), why pay more just for design?

Prof. Dr. Debora Weber-Wulff, FHTW Berlin, FB 4, Treskowallee 8, 10313 Berlin
Tel: +49-30-5019-2320 <http://www.f4.fhtw-berlin.de/people/weberwu/>



Report problems with the web pages to [the maintainer](#)



THE RISKS DIGEST

Forum on Risks to the Public in Computers and Related Systems

ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Volume 22: Issue 98

Monday 27 October 2003

Contents

- [Internet fraud update](#)
[NewsScan](#)
- [Casino barcode forgery](#)
[Steve Dunbar](#)
- [Air Traffic Control vulnerable to fire!](#)
[Paul Cox](#)
- [South Carolina DMV software glitch costs Sumter County \\$164,000](#)
[Frank Carey](#)
- [New risk of leaving devices OFF](#)
[Walter Roberson](#)
- [Mississippi liquor stores and restaurants risk going dry](#)
[Ben Moore](#)
- [RFID friend and foe, with a note on biometric passports](#)
[Markus Kuhn](#)
- [Amazon's new 'search inside the book' feature](#)
[NewsScan](#)
- [Amazon's new text search service](#)
[Drew Dean](#)
- [Google Stumbles?](#)
[Monty Solomon](#)
- [Unwanted e-mail turns into a "chain of stupidity"](#)
[William Colburn](#)
- [Re: Recent London power outage](#)

[Martin Ward](#)

- [Re: First DEWEY DEFEATS TRUMAN, and now YANKEES LOSE!](#)

[Amos Shapir](#)

- [Yet Another eBay-Spoofing Scam](#)

[David Graham](#)

- [Self-inflicted phishing](#)

[Andrew Yeomans](#)

- [SNAFU at the bank](#)

[Walter Regan](#)

- [Re: Top 10 data disasters](#)

[Merlyn Kline](#)

- [Info on RISKS \(comp.risks\)](#)

🔥 Internet fraud update

<"NewsScan" <newsscan@newsscan.com>>

Fri, 24 Oct 2003 08:17:15 -0700

The Federal Trade Commission says that complaints of Internet-related identity theft more than tripled last year, to 2,352 last year from the year

before. Jay Foley of the Identity Theft Resource Center says,

"Online fraud

is becoming as big an issue for eBay and AOL as security is for Microsoft."

Typically, eBay covers buyers or sellers for up to \$200 (or \$500 for some

listings) if an item is not delivered or is in bad condition, though there

is a \$25 processing fee. Posting safety tips for eBay transactions are

listed at www.ebay.com/securitycenter. [**USA Today**, 24 Oct 2003; NewsScan Daily, 24 Oct 2003]

http://www.usatoday.com/tech/news/2003-10-23-fraud_x.htm

🔥 Casino barcode forgery

<Steve Dunbar <stvdnb@yahoo.com>>

Sat, 18 Oct 2003 12:06:20 -0700

The Kalispel Indian Tribe's Northern Quest Casino near Spokane, Washington, lost around \$100,000 to forgers who printed copies of barcoded payout tickets.

<http://www.registerguard.com/news/Wire/N1620WA--CasinoScam.html>

✶ Air Traffic Control vulnerable to fire!

<"Paul Cox" <pcox@eskimo.com>>

Mon, 27 Oct 2003 00:51:34 -0800

I work as an air traffic controller at Seattle Air Route Traffic Control Center. We were less busy than usual today, because nearly all of the flights to/from southern California were severely delayed or canceled.

Not only did the fires in the SoCal area generate large volumes of smoke (reducing visibility and slowing traffic in general) but the fires threatened the physical structure of the main Southern California Terminal Radar Control (SoCal TRACON) facility.

From the controllers' union regional vice president, Bob Marks...

"SCT structurally received minimal damage, but the pine trees at the entrance caught fire and the Fire Department chopped them down so they wouldn't fall into the building. The field next to the facility burned completely.

The facility was full of smoke, and we estimate a minimum of two days before it reopens. The FAA has been great, and honored our request for

air sampling prior to having controllers come back."

The RISK here should be obvious; you've got a facility that is designed and intended to be in operation 24X7, no matter what. They have power backup systems there that can run the TRACON for at least a week on the on-site diesel fuel.

But if the air outside is too smoky from fires in the immediate vicinity, and people cannot work inside the building (apparently it was so smoky inside people were coughing up hunks of lungs... well, not quite, but really bad) then the precautions don't do much good.

Additionally, the physical building itself was threatened with fire damage.

The controllers at the enroute facility (like I work at) in Los Angeles were able to take over the airspace that SoCal TRACON works, but at greatly-reduced traffic rates. Again, from Bob Marks...

"ZLA took over TRACON ops. My deepest gratitude and thanks to the good members at my old facility for dealing with this emergency. The news is not all good, however, as it appears there is pressure to try and run the system "nominally" when the busiest TRACON on the planet is ATC-Zero. A center cannot safely run a significant percentage of approach traffic during a sustained period for several reasons:

Technical: Finals, MVAs, and other map items are not displayed. Mosaic requires 5-mile minimum separation. Radar ID is more cumbersome, since usually the a/c is more than a mile from the departure end of the runway before tag-up.

Training: Most center controllers don't do approach control work, or

haven't for years.

Proficiency: When was the last time you got a thorough briefing and training on ATC-Zero procedures?"

Basically, to maintain the minimum level of safety, controllers had to drastically reduce the numbers of flights from what the TRACON would ordinarily handle.

More RISKS... lack of training, lack of forethought in planning video maps, keeping copies of routes and procedures handy, and some other technical issues (facilities that had a need to talk to one another had to rely on regular commercial telephones, or cellphones, because the FAA doesn't have the proper 24X7 dedicated circuits between all of them).

In the end? Kept the skies safe, as always, but the monster delays (several flights that I personally knew of from Portland, Oregon, and from Seattle, Washington, were delayed by 10+ hours) showed that lack of good contingency planning- and drills on contingency plans- severely hampered the FAA's ability to react to the problems.

✈ South Carolina DMV software glitch costs Sumter County \$164,000

<Frank Carey <Carey1938@aol.com>>
Sat, 25 Oct 2003 20:56:49 EDT

The South Carolina Department of Motor Vehicles says it has sent Sumter County officials a list of nearly 1,000 automobile tax records that were possibly left off the county's tax rolls because of problems with their Project Phoenix software which had been installed last year. In August of

this year Sumter County officials discovered they were missing a large number of car tax records and that the missing records had cost the county \$164,000. When first confronted with the situation in August, DMV officials said they were unaware of any problems with the software. After looking into the Sumter County complaint, the state DMV officials recognized that records might have been omitted but also that the software glitches caused billing problems. Other South Carolina counties have also reported the same problems. [*The Item*, Sumter, SC, front page, 24 Oct 2003]

🚩 New risk of leaving devices OFF

<Walter Roberson <roberson@ibd.nrc.ca>>
Wed, 22 Oct 2003 13:32:12 -0500 (CDT)

Cisco recently announced an unusual problem with leaving some of its devices *off*. It seems that a particular lot of electrolytic capacitors in some of its 2900XL and 3500XL switches undergo chemical degradation when the devices are powered off for extended periods. This can lead to Cyclic Redundancy Check (CRC) and Frame Check Sequence (FCS) errors in the switches.
<http://www.cisco.com/warp/public/770/fn26174.shtml>

[Somehow I never expected quite this form of "bit rot"!]

🚩 Mississippi liquor stores and restaurants risk going dry

<Ben Moore <ben.moore@juno.com>>
Mon, 27 Oct 2003 01:39:35 GMT

Mississippi's Alcohol Beverage Control division shut down the warehouse last week for an indefinite amount of time to fix computer problems, with an estimated outage of at least one week. (Most establishments do not keep more than a week's backlog.) [Source: AP item, PGN-ed]
<http://www.godesoto.com/modules.php?op=modload&name=News&file=article&sid=2313&mode=thread&order=0&thold=0>

✦ RFID friend and foe, with a note on biometric passports

<Markus Kuhn <Markus.Kuhn@cl.cam.ac.uk>>
Sun, 26 Oct 2003 22:28:47 +0000

One is tempted to think of the planned RFID tagging of all US DoD supplies as a major step forward. This will finally enable the design of a new and far safer generation of mines that detonate only near people carrying DoD equipment.

Defense Department drafts RFID policy

Matthew Broersma, CNET News.com

The U.S. Department of Defense will give radio frequency identification technology a massive boost with a new policy requiring its suppliers to use RFID chips. [...]

RFID chips, or tags, contain identification information that can be wirelessly passed on to a reader, allowing, for example, the contents of a shipping container to be identified without opening it. This promises huge improvements in supply-chain efficiency, but also raises the

prospect of remote tracking of consumers via RFID chips embedded in their clothes or the cards in their wallets.

The Defense Department's policy requires that by January 2005 all suppliers embed passive RFID chips in each individual product if possible, or otherwise at the level of cases or pallets. [...]

<http://news.com.com/2100-1008-5097050.html>

But progress will not stop there. With the "US PATRIOT Act" requiring contactless ID chips to be embedded in passports from October 2004, mines and booby-traps will soon also be able to read out remotely the victim's name, age, height, sex and nationality right before triggering, providing an unprecedented reduction in the RISK of killing the wrong person in your next local invasion, terror, anti-terror, or genocide campaign.

A related and more serious note on passport security:

The ICAO radio transmitters about to be added to new passports from later next year on will enable every country on the planet to query the chip's data at a few meters distance (with suitably constructed antennas). Representatives of two German government agencies (BSI, BKA) expressed serious concerns about the security and privacy implications of this in the relevant standards committee. They suggested to use the data on the existing optical character recognition (OCR) stripes in each passport as a code for enabling access to the chip. This way, the passport could only be read by anyone who had already seen its written content before. The idea would be perfectly practical, as the RFID readers at border stations would normally be integrated in the optical readers needed for existing machine-readable travel documents. US representatives, however, have already rejected this quite elegant suggestion in the relevant standards committee.

I suggested at an ISO/ICAO meeting last July in London to add a small metal shield to the front cover page of the passport, such that the RFID coil antenna in the back cover page can work effectively only while the passport booklet is open. Again, this idea was quickly rejected by some of those driving the project as a privacy concern and therefore "of little interest here". But as it is not dependent on any provisions in the chip's internationally standardized protocol, it can still be hoped that responsible passport issuers will implement something along these lines anyway.

<http://www.icao.int/mrtd/>

Markus Kuhn, Computer Laboratory, University of Cambridge
<http://www.cl.cam.ac.uk/~mgk25/> || CB3 0FD, Great Britain

Amazon's new 'search inside the book' feature

<"NewsScan" <newsscan@newsscan.com>>

Fri, 24 Oct 2003 08:17:15 -0700

Amazon.com has announced a new feature called "Search Inside the Book" that is making the text of 120,000 books (more than 33 million pages) fully searchable at no charge. The feature makes it possible to scan a database for the word or phrase entered by a visitor to Amazon's site for each relevant portion of a searchable book. The pages that are found can be read onscreen and printed but not copied or downloaded. University of Washington computer scientist Oren Etzioni says: "It's an impressive feat -- a bold concept, coupled with nice execution and clear business thinking. This really shows Amazon is a technology company, not innovating just with things like free shipping but putting something out there that's brand

new." [Seattle Post-Intelligencer 24 Oct 2003; NewsScan Daily, 24 Oct 2003]

<http://www.siliconvalley.com/mld/mercurynews/business/7092377.htm>

Amazon's new text search service

<Drew Dean <ddean@csl.sri.com>>

Fri, 24 Oct 2003 16:12:01 -0700 (PDT)

Amazon recently announced a new full text search service of 120,000 books:

<http://www.siliconvalley.com/mld/mercurynews/business/7092377.htm>

I decided to try a random search. As "To be or not to be" is a really bad search string (it consists entirely of stop words, that is, words to be ignored by text indexers), I decided on "Call me Ishmael." [For RISKS' international audience, this is the opening line of Herman Melville's Moby Dick, quite possibly the most famous opening line in all of American literature.]

The results are interesting: 2704 books are found, the 1st is "Call me Ishmael," the 2nd is "Call Me Ishmael Tonight: A Book of Ghazals," the 3rd is "The First Five Pages: A Writer's Guide to Staying Out of the Rejection Pile," and the 4th is "Programming Windows with C# (Core Reference)" !!

The highest rated match that directly relates to Moby Dick is the Cliffs Notes at #15. Moby Dick itself isn't in the top 20. <sigh>

Drew Dean, Computer Science Laboratory, SRI International

Google Stumbles?

<Monty Solomon <monty@roscom.com>>

Sun, 19 Oct 2003 01:00:43 -0400

Is Google starting to show signs of strain against spammers and Web scammers?

Chatters at the geek news site Slashdot observed this week that using the search engine to track down certain oddball series of words, such as "speaker bracelet" or "candle truck," turned up strangely low results.

Instead of finding only the expected handful of sites, Google reported

that none could be found. Cambridge, Mass., computer programmer Seth

Finkelstein, an expert on Internet filters, thinks he's figured out the

reason. "The Google search results are crashing, presumably as a result

of a bug in the spam-filtering measures." (See www.sethf.com)

The explanation involves dummy Web sites with long lists of words that are intended to provide matches and then link to Web scammer sites.

[Source: Mike Musgrove, Google Stumbles? Web Watch, 12 Oct 2003, F07; PGN-ed]

<http://www.washingtonpost.com/wp-dyn/articles/A11461-2003Oct11.html>

✶ Unwanted e-mail turns into a "chain of stupidity"

<"Schlake (William Colburn)" <schlake@nmt.edu>>

Mon, 20 Oct 2003 13:50:39 -0600

Several years ago I wrote a print accounting filter for LPRng. In case of a problem it sent e-mail to a list of people here at work. Another department on campus wanted it, so I sent the filter to them. I later remembered (when I started getting e-mail) that there was a hard coded address in it. Attempts to get them to remove or change it proved fruitless, so I

just made
a procmailrc script to mail the error back to them. Today, after a
good two
years of my sending the e-mail back to them, that department
apparently got
fed up, and set up a procmail script of their own which mails me back
a
thank you for each of these messages I forward to them. I added
their thank
you to my spam filter, and I'm blocking them now.

The risk here is a chain of stupidity. I gave out some software that
meant
for in house use. They are using it but are unable or unwilling to
change
an e-mail address in it. I use procmail to push the problem back to
them.
They use procmail to push the problem back to me. I use a Sendmail
milter
to block their e-mail. Another escalation like this and I'll be
hoarding my
precious bodily fluids and calling for Wing Attack Plan R.

✉ **Re: Recent London power outage (Amey, [RISKS-22.97](#))**

<Martin Ward <Martin.Ward@durham.ac.uk>>
Fri, 24 Oct 2003 09:47:59 +0100

It is irrelevant *when* the transformer was switched out.
Transformers are
expected to be switched out occasionally (for either routine
maintenance, or
emergency maintenance). The circuits are designed to take the extra
load
when one or two transformers are switched out. In this case, one
circuit
experienced an extra load which was still well within its design
capacity,
but a relay with the wrong rating (1,020 amps instead of 5,100 amps)
had
been installed on the circuit which tripped while the cable was well

within
its operating capacity of 4,450 amps.

The point is that the accident was waiting to happen from the time the relay was fitted: "basic preventive maintenance" of fixing the leak as soon as it was found would have necessitated switching out the transformer and would also have triggered the power outage.

Martin.Ward@durham.ac.uk <http://www.cse.dmu.ac.uk/~mward/>

✶ Re: First DEWEY DEFEATS TRUMAN, and now YANKEES LOSE!

<amos083@walla.co.il>

Sat, 25 Oct 2003 12:35:40 +0200

A similar error, but much more embarrassing (*) had happened on Ynet, Israel's largest news site (www.ynet.co.il): on the day the Columbia shuttle was lost, at 16:09 local time (09:09 EST) -- the time it was due to land -- an item was released bearing the title COLUMBIA LANDED SAFELY, with some details of what Israel's first astronaut Ilan Ramon was supposed to be doing oafter landing. The item was removed after a few minutes, but apparently not soon enough to be copied and spread around the net for infamy.

* For those of us who consider matters of life and death more important than baseball...

✶ Yet Another eBay-Spoofing Scam

<David Graham <davidg1@cox.net>>

Sun, 19 Oct 2003 13:20:39 -0400

I received an unsolicited e-mail yesterday (one of the hundred or so unsolicited e-mails a day that I am up to now), with this link:

<http://scgi.ebay.com%69%6E%64%65%78%75%70%64%61%74%65%79%6F%75%72%69%6E%66%6F%72%6D%61%74%69%6F%6E%73%65%63%75%72%65%32%31%31%2E%31%34%32%2E%32%32%36%2E%31%36%37:%34%39%38%37/%69%6E%64%65%78%2E%68%74%6D>

followed by several lines of semi-nonsense. The link resolves to 211.142.226.167:34/index.htm

The e-mail included a GIF which, if loaded inline, would display what looks

like a completely legitimate account verification message from eBay, together with a faked link to a (legitimate looking) eBay URL. The real URL

above would not be disabled, however; only covered up. I did not try this,

but I **think** that clicking the faked link would actually load the real one

hidden underneath.

[The attached GIF was deleted. Vastly too long for RISKS. PGN]

I tried to notify eBay but eventually gave that up as too much trouble.

(1) Simply forwarding suspect e-mail to abuse@ebay.com no longer works;

all I got was a bounce directing me to a notification URL.

(2) As always, I had to login to eBay insecurely, just to try to tell them about this new scam.

(3) The notification page, once I got to it, would only accept text.

No

way to send eBay the "faked text" GIF which made this scam noteworthy (and potentially very effective).

Risks:

1. Letting your browser autoload anything other than plain text.
2. Trusting eBay not to be clueless about security.

[Furthermore, this was the first legitimate message to RISKS among

the week's more than 7000 spams. It was the "notsp" that enabled me to spot it. TNX! PGN]

Self-inflicted phishing

<"Andrew Yeomans" <andrew_yeomans@yahoo.com>>

Mon, 27 Oct 2003 22:21:07 -0000

In September I received a newsletter from BT Openworld, which very kindly warned me about "e-mails titled 'From your ISP'. You're asked to download 'new' dial-up software* - this may result in high connection charges". Later on they helpfully offer "if you're worried that you've installed a 'fake' dialer, simply download BT Openworld's ICM dialer to replace it. To do this, click here...".

But the URL provided is

<http://www.digitaldataanalysis.com/btopenworld/r.emt?h=www.btopenworld.com/>

[business/help/sections/0,,1_23_2_0,.html&t=IEiFHQ&e=QJmXtQtyJPQ](http://www.digitaldataanalysis.com/business/help/sections/0,,1_23_2_0,.html&t=IEiFHQ&e=QJmXtQtyJPQ)

The headers of the message also indicate it was sent from "BT Openworld Business Team" <btopenworld@digitaldataanalysis.com>

I tried asking BT Openworld whether

- a) This was a "phishing" scam, or
 - b) They were incapable of running URL click tracking themselves.
- Unfortunately their help desk was unable to give me a definitive answer, as e-mail bounced ("mailbox full") when I tried to forward the original e-mail.

Not to be outdone, Smile on-line bank in their October newsletter say "To

find out more about the recent e-mail scam affecting various UK banks, visit

<http://www.smile.co.uk>". But the URL at the end is actually

<http://www.foretelsystems.com/eventmonitor/monitor.aspx>

?cn=76&id=6936&ev=12&rd=http://www.smile.co.uk
This had Return-Path: <bounce@foretelsystems.com>

At least their help desk could assure me "The e-mail that you attached is a genuine e-mail, and has not been spoofed. Fortel systems handle the smile marketing e-mails."

So how can I tell whether future e-mails are genuine?

A case of "Give a man a phish; you might catch account details today. Teach a man to phish; and you have been caught for a lifetime".

Andrew Yeomans, 65 Grove Road, Tring, Herts, HP23 5PB, UK
andrew_yeomans@yahoo.com

✶ SNAFU at the bank

<"Walter Regan" <regan@comnet.ca>>
Thu, 23 Oct 2003 21:51:50 -0400

On my way to work this (Thursday) morning, I heard a news item on the radio concerning a drive-thru ATM machine at a bank. It was reported that, over the last weekend, at least one customer had had his bank account drained by someone who had installed a 'skimmer' over top of the card reader to copy customers' ATM cards and a pinhole camera to capture customers' P.I.N. numbers.

I found this story of particular interest because my wife had used that very ATM machine on Sunday morning. So I decided to call the bank to see if my wife's ATM card had been compromised. I dialed the number for what is laughably called 'customer service'. An automated voice read a menu to me detailing what information I could obtain by selecting one, two and

three

and then went on to say that, if I really wanted to talk to a customer service representative, I should select zero. I selected zero and, after a short pause, I got a busy signal.

I decided to try again. This time I thought I might be able to preempt the menu by selecting zero before it was finished. No such luck. As soon as I selected zero, an automated voice, (which sounded very disappointed with me), told me that I had made an invalid selection and the menu spiel restarted from the beginning. So I waited until it had finished, selected zero and got a busy signal again.

As it appeared that it would involve a long and frustrating ordeal to contact the bank in question, I instead phoned the main branch of the same bank. Surprisingly, a very obliging human being answered and, after I had explained the problem, gave me the unlisted phone number of the manager at the bank in question. I phoned this number, which got me to an answering machine. I left my phone number and a brief description of the problem.

Hours later, I received a phone call from someone (not the manager) at the bank in question. She said that my account did not seem to have been tampered with. I asked if they could tell from the surveillance cameras when the skimmer had been removed. She told me that the surveillance cameras transmit the pictures directly to a central location in another city so that they had no way to tell how long the skimmer had been installed. She said that, for my own peace of mind, I could replace the ATM card or change the P.I.N. number.

Several RISKS present themselves here - the vulnerability of the ATM machines to the skimmer , the poorly designed automated answering

system,
the bureaucracy that centralizes the capture of data but apparently
cannot
analyze it in a timely fashion, the lackadaisical attitude.

✉ Re: Top 10 data disasters ([RISKS-22.96](#))

<"Merlyn Kline" <merlyn@zyweb.com>>

Mon, 20 Oct 2003 10:24:42 +0100

> This could be a result of the rush to complete work and leave early
for
> the weekend on Friday afternoons, as well as a lack of staff
concentration
> on Monday mornings,"

Or perhaps it could be a result of the fact that many of these cases
are
precisely **not** those where human error is to blame -- computer
failure
often occurs in machines running 24x7 so, given a reasonably even
distribution, around 35% of such failures will occur at the weekend
and not
be discovered until Monday morning when the users arrive to discover
their
data loss and ask for assistance with recovery. This will obviously
give
rise to a peak in recovery activity on Mondays. Recovery "experts"
should be
very familiar with this.

[...] Recovery "experts" should not be amazed by the fact that a
physically
damaged computer often does not contain a completely destroyed hard
drive.

RISKS readers should not be amazed to see yet another marketing
press-release reproduced as "news", even on the BBC site. For the
same to
make it into RISKS is another thing altogether...



Report problems with the web pages to [the maintainer](#)