



# 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 21: Issue 1

**Tuesday 15 August 2000**

## Contents

- [Russian nuclear sub trapped on bottom of Barents Sea](#)  
[Keith A Rhodes](#)
- [Risks of train doors: Sydney](#)  
[Simon Carter](#)
- [Admissions mixup leaves Northeastern University struggling](#)  
[Daniel P. B. Smith](#)
- [Not so smart weapons in Kosovo](#)  
[Lord Wodehouse](#)
- [Private phone records on Web](#)  
[Kevin L. Poulsen](#)
- [Barclays Internet-banking security-glitch following software upgrade](#)  
[Pete Morgan-Lucas](#)
- [Security hole in Netscape](#)  
[NewsScan](#)
- [The Pentagon worries that spies can see its computer screens](#)  
[Gregory F. March](#)
- [Online gambler goes to prison](#)  
[NewsScan](#)
- [County blew \\$38 million on canceled payroll system!](#)  
[Joan Brewer](#)

- [Delays in the new UK Air traffic control system](#)  
[Ursula Martin](#)
  - [Microsoft vulnerabilities, publicity, and virus-based fixes](#)  
[Bruce Schneier](#)
  - [REVIEW: "NT 4 Network Security", Strebe/Perkins/Moncur](#)  
[Rob Slade](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

## ✶ Russian nuclear sub trapped on bottom of Barents Sea

"Keith A Rhodes" <rhodesk.aimd@gao.gov>

Mon, 14 Aug 2000 07:22:26 -0400

A Russian nuclear submarine malfunctioned while on exercises, and was trapped on 13 Aug 2000 on the bottom with a crew of more than 100 aboard.

[There was not much hope for the crew.]

[\*Izvestia\* reported recently that, according to the most conservative estimate, 507 submarine crew members have died during the 40-year history of Russian nuclear submarines, not counting this one.]

[Source: Article by Barry Renfrew, Associated Press, 14 Aug 2000; PGN-ed]

[I think the most telling line in this report is that the Russian Navy is in a shambles with their vessels getting no regular maintenance. Seems that in this case the tables have turned -- usually everyone is complaining about not keeping up with their software maintenance, although I guess that if they did not maintain the vessel's mechanical systems, they did not maintain its computer systems. Keith]

## ✶ Risks of train doors: Sydney

Simon Carter <smjc@svrc.uq.edu.au>

Tue, 01 Aug 2000 13:57:36 +1000

This is the latest in a series of disasters and irritants on the Sydney train system:

> As a commuter, Mr Dee almost became a victim of the system he supported  
> when his leg became trapped in a train door as it left Meadowbank Station  
> on Sunday afternoon.

<http://www.smh.com.au/news/0008/01/text/national3.html>

A colleague suggested:

> This one's almost worth sending to RISKS forum. Train doors have a long  
> history of hazardous action (or inaction, as in this case).  
>  
> Off the top of my head:  
>  
> For a long time, Brussels metro had no automatic opening mechanism, so  
> that anything trapped in a closing door stayed trapped. It sounds like  
> Sydney used the same contractor.  
>  
> Calgary did install an opening mechanism, but the sensors failed when  
> the rubber door seals hardened at -30C.  
>  
> More amusingly, a woman jumped onto the London U/G, except the doors  
> shut on her handbag. "No worries, I'm getting off next stop, I'll get it

> back then." The doors opened on the other side of the carriage.  
>  
> There's a story somewhere about a computer-controlled train  
> persistently stopping out of alignment with doors on the  
platform edge.  
>  
> 'Fraid I can't give a reference for any of these.  
>  
> David

[David Tombs <Tombs@svrc.uq.edu.au>]

I recall there were numerous problems with the Bay Area BART system when it first went into service (mid '70's?). All sorts of things including doors opening while traveling between stations.

Simon Carter <smjc@svrc.uq.edu.au>

[Lots of rail problems in the RISKS archives. See <http://www.csl.sri.com/neumann/illustrativerisks.html> and click on Rail, Bus, and Other Public Transit in the index. PGN]

---

## **Admissions mixup leaves Northeastern University struggling**

"Daniel P. B. Smith" <dpbsmith@bellatlantic.net>

*Thu, 10 Aug 2000 05:56:43 -0400*

After problems with its new computer system, Northeastern University unintentionally admitted 25 percent too many freshmen -- 600 extra students -- for this fall. Earlier, the names of hundreds of potential applicants had been lost when the system was first installed, which resulted in an

aggressive campaign to enroll the students who had been accepted. [Source: \*The Boston Globe\*, 10 Aug 2000; PGN-ed]

Daniel P. B. Smith, 35 Mountain Ave, Norwood, MA 02062  
dpbsmith@bellatlantic.net (Lifetime address: dpbsmith@mit.alum.edu)

[Also noted by Dave Bank. PGN]

---

## ✶ Not so smart weapons in Kosovo

Lord Wodehouse <w0400@bigfoot.com>

*Mon, 14 Aug 2000 13:23:02 +0100*

Yet again there is any report on smart weapons, actually not being as smart as portrayed by the military. It is so like the hype of the Patriot missile (various issues of RISKS [and the illustrativerisks.html archive]). This survey was carried out by Flight International and the BBC radio Today programme. [http://news.bbc.co.uk/hi/english/uk/newsid\\_879000/879560.stm](http://news.bbc.co.uk/hi/english/uk/newsid_879000/879560.stm)

The risks are again obvious. The computer game warfare style does not deliver what it is meant to do so, but the military continues to pursue it, because they can get more money that way.

The prospects for the NMDS (son of Star Wars) looks even more unrealistic in this light. I strongly believe that we all need a good dose of reality in relation to what technology and computers can do, and where other factors,

such as the weather limits the optimistic expectations.

Global Research Information Systems, Glaxo Wellcome, Stevenage  
SG1 2NY UK  
+44 1438 76 3222 w0400@ggr.co.uk [http://ds.dial.pipex.com/  
lordjohn/](http://ds.dial.pipex.com/lordjohn/)

---

## ⚡ Private phone records on Web

"Kevin L. Poulsen" <klp@securityfocus.com>  
*Mon, 14 Aug 2000 11:11:07 -0700 (PDT)*

<http://www.securityfocus.com/news/074>

Verizon's twenty-eight million residential and business telephone subscribers from Maine to Virginia had portions of their private telephone records exposed on a company web site, SecurityFocus has learned.

The telephone giant, already struggling in a strike by union workers, was scrambling Sunday night to shut down the offending web application: a system designed to allow customers to file new repair reports, and track existing reports, over the Internet. Because of a basic design flaw, users could put in any phone number in Verizon's northeastern U.S. service area, and, by viewing the source of the resulting page, see the owner's name and address, as well as other information.

"We're going to have to go to a fix, obviously," said company spokesperson Larry Plumb, who learned of the flaw through SecurityFocus's inquiry. "We won't open up that application again until we have the

problem solved."

Kevin L. Poulsen, Editorial Director, SecurityFocus.com,  
Washington D.C.  
(202)232-5200

---

## ✂ **Barclays Internet-banking security-glitch following software upgrade**

Pete Morgan-Lucas <pjml@nsgmail.nerc-swindon.ac.uk>  
*Tue, 1 Aug 2000 09:30:44 +0100 (BST)*

Barclays Bank yesterday had a problem with their online banking service - at least four customers found they could access details of other customers. Barclays are claiming this to be an unforeseen side-effect of a software upgrade over the weekend.

See [http://news.bbc.co.uk/hi/english/business/newsid\\_860000/860104.stm](http://news.bbc.co.uk/hi/english/business/newsid_860000/860104.stm) for more details.

//Pete Morgan-Lucas// NERC\_ITSS Network Security, NERC Swindon.

[Also noted by AllyM at <http://www.theregister.co.uk/content/1/12287.html>

and Andrew Brydon in a BBC item that mentioned 7 complaints.  
PGN]

---

## ✂ **Security hole in Netscape**

"NewsScan" <newsscan@newsscan.com>

*Tue, 08 Aug 2000 07:32:18 -0700*

Because of a security hole in the Netscape browser, about a thousand computers have been infected in a way that would allow a network vandal to see, run, and delete files on the victim's computer. Netscape is working rapidly to solve the problem, but network security experts are suggesting that, until the solution is found, Netscape users should disable the Java programming languages in their browsers. [AP/\*Los Angeles Times\*, 6 Aug 2000, <http://www.latimes.com/business/cutting/20000808/t000074055.html>; NewsScan Daily, 8 August 2000]

---

## **⚡ The Pentagon worries that spies can see its computer screens**

"Gregory F. March" <march@gfm.net>

*Thu, 10 Aug 2000 08:59:11 -0400*

There was a front page article in the \*Wall Street Journal\* (7 Aug 2000) discussing the technology and risks of video-screen snooping by scanning the EMF radiated by the monitor.

I'm not an engineer, but I can put two and two together. I have a wireless keyboard and mouse. If someone could view my monitor remotely and then send the appropriate commands to my Logitech mouse/keyboard, it could be a \*huge\* potential risk for leaving my machine on and unattended.

Gregory F. March      ---      <http://www.gfm.net/~march>      ---

AIM:GfmNet

---

## ✂ Online gambler goes to prison

"NewsScan" <newsscan@newsscan.com>

*Fri, 11 Aug 2000 09:53:55 -0700*

A co-owner of an online offshore gambling business based on the Caribbean island of Antigua has been sentenced to 21 months in a U.S. prison for violating this country's federal Wire Wager Act, which makes it illegal to use telephone lines in interstate or foreign commerce to place sports bets.

The prosecutor noted: "An Internet communication is no different than a telephone call for purpose of liability under the Wire Wager Act."

[Reuters/\*The New York Times\*, 11 Aug 2000; NewsScan Daily, 11 August 2000;

<http://partners.nytimes.com/library/tech/00/08/biztech/articles/11gambling.html>]

---

## ✂ County blew \$38 million on canceled payroll system!

"Joan Brewer" <pegasus@transport.com>

*Mon, 31 Jul 2000 07:44:08 -0700*

The managers of King County's unfinished \$38 million Financial Systems

Replacement Program (FSRP) computer system did not use basic computer and

business procedures, forcing part of the system online before it

was ready,  
spending the rest of their budget trying to fix the resulting  
problems, and  
leading to the cancellation of the project, largely because of  
delays and  
cost overruns in the payroll system for the county's 19,000  
employees. The  
resulting system reportedly can handle only one-third of the  
load. [Source:  
Article by Roberto Sanchez, County blew \$38 million: Here's what  
went wrong,  
\*The Seattle Times\*, 28 July 2000; PGN-ed]

---

## ✦ **Delays in the new UK Air traffic control system (Re: [RISKS-20.93,94](#))**

Ursula Martin <ursula@csl.sri.com>  
*Thu, 10 Aug 2000 10:41:39 -0700*

400 technicians (software engineers perhaps?) have reduced the  
number  
of [known] bugs from 500 to 200 in recent weeks.  
[See [http://news.bbc.co.uk/hi/english/uk/newsid\\_873000/873765.stm](http://news.bbc.co.uk/hi/english/uk/newsid_873000/873765.stm)]

---

## ✦ **Microsoft vulnerabilities, publicity, and virus-based fixes**

Bruce Schneier <schneier@counterpane.com>  
*Mon, 07 Aug 2000 09:07:45 -0500*

The latest tale of security gaps in Microsoft Corp.'s software  
is a  
complicated story, and there are a lot of lessons to take

away ... so let's  
take it chronologically.

On June 27th, Georgi Gunniski discovered a new vulnerability in Internet Explorer (4.0 or higher) and Microsoft Access (97 or 2000), running on Windows (95, 98, NT 4.0, 2000). An attacker can compromise a user's system by getting the user to read an HTML e-mail message (not an attachment) or visit a website.

This is a serious problem, and has the potential to result in new and virulent malware. But it requires Microsoft Access to be installed on the victim's computer, which, while common, is by no means universal. A virus that exploits this vulnerability will not spread as widely as, say, Melissa. In any case, Microsoft published a fix on July 14th, and I urge everyone to install it.

On July 17th, SANS promulgated an e-mail warning people of the "most dangerous flaw found in Windows workstations." I can't really figure this e-mail out; it seems to be primarily a grab for press coverage. Some of it is suspiciously vague: "We developed this exploit further and realized that this is one of the most serious exploits of Windows workstations in the last several years" "Developed"? How? No one says. Some of it brags: "Microsoft asked us not to release the details until they had a fix." "Release the details"? But the original Bugtraq posting was pretty explanatory, and SANS has not released anything new.

Still, the SANS e-mail received a lot more publicity than the

Bugtraq

announcement or the Microsoft patch, so it's hard to complain too much.

But the SANS announcement had a much more disturbing section:

"It may be

possible to fix this vulnerability automatically, via an email without

asking every user to take action. The concept is similar to using a

slightly modified version of a virus to provide immunity against infection.

SANS is offering a \$500 prize (and a few minutes of fame) to the first

person who sends us a practical automated solution that companies can use,

quickly, easily, and (relatively) painlessly to protect all vulnerable

systems." (This paragraph is no longer on the website, which claims that

"winning entries have been received.")

This is a really, really dumb idea, and we should put a stop to this kind

of thinking immediately. Every once in a while someone comes up with the

idea of using viruses for good. Writing a virus that exploits a particular

security vulnerability in order to close that vulnerability sounds

particularly poetic.

First, there's no audit trail of the patch. No system administrator wants

to say: "Well, I did try and infect our systems with a virus to fix the

problem, but I don't know if it worked in every case."

Second, there's no way to test that the virus will work properly on the

Internet. Would it clog up mail servers and shut down networks? Would it

properly self-destruct when all mail clients were patched? How

would it  
deal with multiple copies of itself?

And third, it would be easy to get wrong and hard to recover from. Experimentation, most of it involuntary, proves that viruses are very hard to debug successfully. Some viruses were written to propagate harmlessly, but did damage because of bugs in their code. Perfectly intentional experimentation proves that in your average office environment, the code that successfully patches one machine won't work on another, sometimes with fatal results. Combining the two is fraught with danger. Every system administrator who's ever automated software distribution has had the "I just automatically, with the press of a button, destroyed the software on hundreds of machines at once!" experience. And that's with systems that you can \*stop\*; self-propagating systems don't even let you shut them down when you find the problem.

In any case, the SANS announcement was made even more confusing by the announcement of another Microsoft vulnerability at the same time...one that I think is even more serious than the one SANS publicized. (The vulnerability was first discovered on July 2nd, but was independently discovered and published on Bugtraq on July 18th.)

A buffer overflow in Microsoft Outlook or Outlook Express allow an attacker to execute arbitrary code on a victim's machine just by sending him an email. In Outlook Express, the victim doesn't even have to open the email, or preview it. All he has to do is download it. In Outlook, he has to read it.

That's the bad news. The good news is that it only is a vulnerability for users who have POP or IMAP installed; those using Outlook's default corporate configuration are not vulnerable. (Home users who link to commercial ISPs are much more likely to be vulnerable.) So again, a virus that exploits this vulnerability would be dangerous and unpleasant, but would not spread unchecked.

Microsoft has a fix. Originally (on July 18th) it required you to upgrade your version of Outlook or Outlook express, but two days later Microsoft did the right thing and issued a patch for all versions. SANS issued another e-mail on July 21st, with more dire warnings: "Please fix this before you go home today. And if you have gone home, go back to the office and fix it." In my opinion, this warning blew the threat completely out of proportion, and was irresponsible to send. SANS made it sound like a virus attack already in progress, not a new vulnerability that someday might be exploited. And right on the heels of the previous warning, it got lost in the noise. When I received the second SANS e-mail, I thought it was another reminder for the first vulnerability. I'll bet that many users were similarly confused, and ignored it as well.

There are several lessons here.

1. Computer programs have two sorts of vulnerabilities, nicely illustrated by these two attacks. First, they have vulnerabilities connected to the basic design of the operating system they run on and the way it

chooses to interlink programs; the Access attack demonstrates this. Second, they have vulnerabilities based on coding mistakes; the buffer overflow problem is an example.

2. It's not enough to release a patch. The press often gets this wrong. They think the sequence is: vulnerability publicized, patch released, security restored. In reality, it doesn't work that way. You don't regain security until you install the patch. Even though both of these vulnerabilities have been patched, I predict attack tools that use them. Many users just won't bother installing these patches. For publicizing the two vulnerabilities, SANS is to be commended.

3. Sensationalizing vulnerabilities will backfire. Both of these vulnerabilities are serious, but neither is monumental. Calling something "the most dangerous flaw" leads people to trivialize other flaws. I worry about the public being completely unable to determine what is important. We've seen viruses that fizzle, and others that run rampant. We've seen vulnerabilities that look serious but don't amount to anything, and ones that are trivial and exploited again and again. SANS needs to be a voice of reason, not of hyperbole.

4. Writing a virus to exploit a vulnerability is a bad idea, even if the goal of that virus is to close that vulnerability. Viruses, by their very nature, spread in a chaotic and unchecked manner; good system administration is anything but.

5. There are still lots of serious vulnerabilities in Microsoft

products,  
and the interactions between products, waiting to be discovered.

The Access/IE vulnerability:

<<http://www.securityfocus.com/bid/1398>>

<[http://www.computerworld.com/cwi/story/0,1199,NAV47\\_STO47273,00.html](http://www.computerworld.com/cwi/story/0,1199,NAV47_STO47273,00.html)>

The SANS announcement:

<[http://www.sans.org/newlook/resources/win\\_flaw.htm](http://www.sans.org/newlook/resources/win_flaw.htm)>

Microsoft's "work around":

<<http://www.microsoft.com/technet/security/bulletin/MS00-049.asp>>

The Outlook vulnerability:

<<http://www.securityfocus.com/bid/1481>>

Reports on the vulnerability:

<<http://www.securityfocus.com/news/62>>

<[http://www.computerworld.com/cwi/story/0,1199,NAV47\\_STO47323,00.html](http://www.computerworld.com/cwi/story/0,1199,NAV47_STO47323,00.html)>

Microsoft's fix:

<<http://www.microsoft.com/windows/ie/download/critical/patch9.htm>>

<<http://www.microsoft.com/technet/security/bulletin/ms00-043.asp>>

This article originally appeared in:

<<http://www.zdnet.com/zdnn/stories/comment/0,5859,2609398,00.html>>

Bruce Schneier, CTO, Counterpane Internet Security, Inc. Ph:  
408-556-2401  
3031 Tisch Way, 100 Plaza East, San Jose, CA 95128 Fax:  
408-556-0889

---

**⚡ REVIEW: "NT 4 Network Security", Strebe/Perkins/Moncur**

Rob Slade <rslade@sprint.ca>

*Mon, 14 Aug 2000 09:14:54 -0800*

BKNT4NSC.RVW 20000609

"NT 4 Network Security", Matthew Strebe/Charles Perkins/  
Michael G. Moncur, 1999, 0-7821-2425-9, U\$49.99  
%A Matthew Strebe ntsecurity@starlingtech.com  
%A Charles Perkins ntsecurity@starlingtech.com  
%A Michael G. Moncur mgm@starlingtech.com  
%C 1151 Marina Village Parkway, Alameda, CA 94501  
%D 1999  
%G 0-7821-2425-9  
%I Sybex Computer Books  
%O U\$49.99 800-227-2346 Fax: 510-523-2373 info@sybex.com  
%P 940 p. + CD-ROM  
%T "NT 4 Network Security, Second Edition"

While dauntingly thick, this is a generally readable, and fairly comprehensive, introduction to security in general, and particularly to Windows NT in a networked environment. On the other hand, it sometimes has less material than you would expect.

Chapter one presents a general overview of security, touching lightly on a range of topics and indicating areas the book is going to cover. It is interesting to note that one subject seems to be left out: data and business recovery is only mentioned tangentially. For example, the NTFS disk format is noted to fully support security, but the possible problems in recovering when the disk goes bad are not mentioned. Human security, in chapter two, covers a wide range of social factors, including an extensive discussion of password choice, and the importance of treating your employees fairly and well. The explanation of encryption, in chapter three, deals with a number

of important aspects, but is poorly structured. It also brings in a number of unrealistic factors, such as the use of quantum computers, and neglects some fairly important current developments. A general plan for administering security is proposed in chapter four.

Chapter five presents the Windows NT security model, and, while it does a better job than many other such works, it does not really provide a clear working picture. User account functions, with another look at passwords, is reviewed in chapter six. System policy is introduced in chapter seven, but the overall operation and effect is not explained well, and the material almost immediately degenerates into a terse listing of policy options. Although chapter eight purports to examine file systems, most of it deals with setting security permissions with NTFS.

Chapter nine starts to look at networking issues with workgroups and shares. Unfortunately, while the mechanics of sharing operations are clear enough, the concepts are not. Domains and trust relationships are introduced, but not very functionally, in chapter ten.

Fault tolerance, in chapter eleven, gives some basic information on various types of disk redundancy, and a few tips on backup.

Chapter twelve talks about virus protection. I am used to security texts that have numerous mistakes in this area, but I was astonished to see, at the beginning of this section, mention of a "CMOS virus" (no such thing) that infects the CMOS BIOS code. A computer's "CMOS" is the term used to

refer to the small chip containing battery supported memory, holding a small table of information. This information is used by the BIOS programming, which programming is generally stored in read-only memory. (The next page actually mentions this.) CMOS memory is generally too small to hold any effective virus. In addition, it is only called as data, and no program that you did manage to store in the CMOS area would ever run. In any case, the text goes on to say that these viruses can obtain complete control over a computer, and cannot be removed by most antiviral software. (I suppose the statement about removal is true enough: since they don't exist, who would bother to write removal programs?) There is also an erroneous account of the Brain virus, a two page exegesis on Java that finally admits Java can't be used to create viral applets, a statement that NT is "immune" to file viruses (it's not), a list of antiviral types that only mentions different types of scanners (never mentioning activity monitors or change detection software), and a section on trojan software.

Remote access actually starts with a brief mention, at the end of chapter twelve, of the dangers of pcAnywhere. (Both here and in the following, there are stories of scanning local networks from home ISP service. The authors do not mention that this operation is restricted to those with cable modems.) Chapter thirteen starts off with some opining on phone phreaking, but then does move on to some reasonable information on securing dial-in situations. The material on multi- vendor networks, in chapter

fourteen,  
does little more than assert that other operating systems have  
security  
holes, too, you know! Chapter fifteen is an introduction to the  
Internet,  
but, because of a rather loose structure, does not present  
security concepts  
in a coherent manner. Similarly, the overview of TCP/IP, in  
chapter  
sixteen, lists a number of potential problems with the protocols  
but not  
much instruction on what to do about them.

Chapter seventeen describes a rather random bag of advice on  
security  
aspects on client (non-server, or, in other words, user)  
machines. Then we  
move back into network territory with a blend of firewall and  
virtual  
private network (VPN) technology in chapter eighteen. Chapter  
nineteen  
tells us about VPNs, with a few mentions of firewalls.  
Microsoft BackOffice  
is reviewed in chapter twenty, but without much specific  
information about  
security.

Chapter twenty one lists a variety of user (application) level  
security loopholes. A number of attacks available at the network  
level are listed in chapter twenty two. "The Secure Server," in  
chapter twenty three, looks primarily at physical security and  
concerns (and finally admits that NTFS can be bypassed after  
all).  
Chapter twenty four looks at physical matters again, mostly in  
the  
TEMPEST realm (and with a little misinformation about fibre  
optics and  
fish tanks).

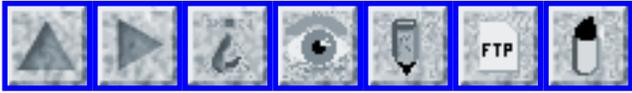
The authors have tried to lighten up a rather heavy topic by  
including  
humour in the text. While the remarks don't really get in the  
way of the

content, they don't really support it, either. There is also an attempt to keep readers from getting lost in the jargon by providing "terminology" boxes throughout the book. This is helpful, but is not used as consistently as it could be. Acronyms, in particular, frequently start to appear in the text without ever having been specifically defined.

This work has better conceptual coverage than "Microsoft Windows NT 4.0 Security, Audit, and Control" by James G. Jumes et al, (cf. BKWNTSAC.RVW), and is about equal to "Windows NT Server 4 Security Handbook" by Hadfield, Hatter, and Bixler (cf. BKNT4SHB.RVW). There is better structure and more willingness to discuss flaws than is apparent in the "Windows NT Security Guide" by Stephen A. Sutton (cf. BKWNTSCG.RVW). It has perhaps the same level of quality, and is certainly larger than "Windows NT Security" by Charles B. Rutstein (cf. BKWNTSEC.RVW), but there is not as much depth in places. "PCWeek Microsoft Windows NT Security," by Lambert and Patel (cf. BKPWNTSG.RVW), has better material in significantly less space. In terms of Internet material, it is about the same as "Internet Security with Windows NT," by Mark Joseph Edwards (cf. BKINSCNT.RVW), although it could hardly be worse. In general it is a good, useful guide, but there are still a number of holes to patch.

copyright Robert M. Slade, 2000 BKNT4NSC.RVW 20000609  
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/>



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 21: Issue 2

**Saturday 26 August 2000**

## Contents

- [Hoaxes: When will they learn?](#)  
[Dave Farber](#)
- [NY State's running out of fingerprint IDs](#)  
[Danny Burstein](#)
- [Mobile phone malware on i-mode in Japan](#)  
[Kevin Connolly](#)
- [Firepower via Web interface](#)  
[Anatole Shaw](#)
- [Sydney Airport baggage system fails for second time in five days](#)  
[Stellios Keskinidis](#)
- [Airline E-Ticket risks](#)  
[Paul Wallich](#)
- [Risks on public transit: mechanical and human failures in Toronto](#)  
[Stephen van Egmond](#)
- [Bangkok robot security guard](#)  
[Torrey Hoffman](#)
- [Professor stole 40 student SSNs and IDs to get credit cards](#)  
[Joan L. Brewer](#)
- [Kaiser Permanente medical e-mails go astray](#)  
[Sheri Alpert](#)

- [Wake up, your TV is talking to your bracelet](#)  
[NewsScan](#)
  - [SSL Server Security Survey](#)  
[Monty Solomon](#)
  - [\\*The Globe and Mail\\* Web site exposing search-engine log file](#)  
[Esteban Gutierrez-Moguel](#)
  - [Blocked e-mail and Web sites](#)  
[PGN](#)
  - [Major security hole in new online organizer service](#)  
[Paul van Keep](#)
  - [Hackers breach Firewall-1](#)  
[PGN](#)
  - [GAO says EPA's computer security is "riddled" with weaknesses](#)  
[Declan McCullagh](#)
  - [Bruce Schneier's Secrets and Lies](#)  
[PGN](#)
  - [Software Risk Management Conference ISACC](#)  
[Gary McGraw](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

## ⚡ Hoaxes: When will they learn?

Dave Farber <farber@cis.upenn.edu>

*Fri, 25 Aug 2000 14:24:13 -0400*

We have had the technology to do digitally signed authentication for many years and yet still companies and people do not sign their email and look what happens, and I mean REAL signatures not just what the Congress thinks is digitally signed material. Dave

Shares of the Emulex Corporation plunged more than 60 percent Friday following the distribution of a bogus press release about the computer

network equipment maker's earnings. Trading in the stock was halted for about three hours after the hoax started showing up in financial news reports. The hoax wiped more than \$2 billion off the company's stock market value, leaving it around \$2 billion.

Emulex's shares finally resumed trading at 1:30 p.m. Eastern time and recaptured most of their loss. The stock was lately trading down 6, or 5.3 percent, at 107 1/16 after earlier plunging as low as 43.

The fake press release, which appeared on the Internet around the time of the market's opening bell, claimed that Emulex would restate its fiscal fourth-quarter earnings as a loss. There were also headlines that the Securities and Exchange Commission was investigating accounting irregularities at the company and that Emulex's president and chief executive, Paul Folino, was stepping down.

[Source: <http://www.nytimes.com/2000/08/25/news/financial/25tsc-emulex.html> (N.B. Link is not valid!!)]

From Dave Farber's IP list.

See also <http://cnfn.cnn.com/2000/08/25/companies/emulex/> .  
PGN]

---

## NY State's running out of fingerprint IDs

danny burstein <dannyb@panix.com>

Sat, 26 Aug 2000 01:44:20 -0400 (EDT)

In a problem officials are comparing to the Y2K scare, the state says

it will run out of numbers to assign to the fingerprints it

keeps on

file -- and will begin recycling old ones -- next year.

[Source: State's running out of fingers to count IDs on,  
by Greg Wilson, \*NY Daily News\*, 25 Aug 2000]

The article continues by pointing out that there are only seven digits for

the ID field, meaning a total of 9,999,999 records. (I'd be a bit surprised

if they had actually started with "0000001" rather than "1000001", but since

these date from the old paper card days it's quite possible.).

With NYS's population being about 18 million (subject to whether you use the

"actual enumeration" census figures or the "statistical correction" - but

that's another Risk entirely...) and with records going back for decades,

the justice division is rapidly running out of numbers.

So, effective in August 2001, they anticipate reusing ID numbers of people

who have died or otherwise been removed from the register.

No need to worry if your ID number matches that of a serial murderer,

though. The article continues that:

Officials offered assurances that the numbers crunch will not result

in the misidentification of law-abiding citizens who are issued

numbers previously assigned to criminals.

Why am I not reassured?

---

## 🔥 Mobile phone malware on i-mode in Japan

<kmc@eircom.net>

*Fri, 25 Aug 2000 08:25:13 +0100*

The risk is that people designing new mobile phone functions do not learn from the mistakes in the MS Word macro "virus enabling" feature.

<http://www.zdnet.co.uk/news/2000/31/ns-17205.html>

"Hundreds of Japanese i-mode users were stung by a prank which forced phones to dial "110" -- the police emergency telephone number in Japan -- during an online quiz."

Kevin Connolly

---

## **⚡ Firepower via Web interface**

Anatole Shaw <anatole@mindspring.com>

*Thu, 17 Aug 2000 19:44:36 -0400 (EDT)*

[http://www.bangkokpost.net/170800/170800\\_News03.html](http://www.bangkokpost.net/170800/170800_News03.html)

The Thailand Research Fund has unveiled a new robot, resembling a giant ladybug with a couple of extra limbs. The unit is equipped with visible-spectrum and thermal vision, and a gun. According to Prof. Pitikhet Suraksa, its shooting habits can be automated, or controlled "from anywhere through the Internet" with a password. The risks of both modes are obvious, but the latter is new to this arena. Police robots of this ilk have been around for a long time, but are generally radio-controlled. The apparent goal here is to make remote firepower available on-the-spot from around the Internet, which means insecure clients everywhere. How long will it take for one of these passwords to be leaked via a keyboard

capture, or a browser bug? Slowly, we're bringing the risks of online banking to projectile weaponry.

---

## **✶ Sydney Airport baggage system fails for second time in five days**

stellios keskinidis <stellios@ozemail.com.au>  
*Sun, 20 Aug 2000 19:07:17 +1000 (EST)*

As a result of an hour-long computer glitch during the integration of the security system with the main baggage-handling system, Sydney airport's new \$43 million baggage system failed on 20 Aug 2000 for the second time in five days (with the Olympic Games a month away). (The previous problem was in the new checked bag screening system.) [Source: PGN-ed from [http://news.ninemsn.com.au/01\\_national/story\\_8815.asp](http://news.ninemsn.com.au/01_national/story_8815.asp), 20 Aug 2000]

[Same article also noted by Steve Gillanders. PGN]

---

## **✶ Airline E-Ticket risks**

Paul Wallich <pw@panix.com>  
*Tue, 1 Aug 2000 16:39:31 -0400*

Continental Airlines has installed a very efficient new system for travelers whose tickets exist only in computerized form: swipe a credit card or other means of ID, tell the touch screen how many bags you have to check and

answer the usual security questions about who packed them and whether they've been out of your sight, and it prints out a boarding pass. You can also change your seat and (possibly) other aspects of your itinerary on the spot.

The machines are supposed to be tended by agents who check your luggage (should you have any to check) and look at a photo ID to make sure you're who your credit card says you are. But in some busy airports (say, for example, Detroit last weekend) the machines appear to function unmonitored.

There's a long list of risks here relating both to terrorism and to theft, and I don't see any obvious way of fixing them in the context of the current system, except perhaps to require an ID check somewhere downstream of the boarding pass issuance.

(Of course it doesn't make me any happier to note that with the endemic delays in today's air transport system you also have passengers leaving aircraft and then reboarding with no verifiable checks on either identity or luggage.)

Paul Wallich

[pw@panix.com](mailto:pw@panix.com)

---

## **✶ Risks on public transit: mechanical and human failures in Toronto**

Stephen van Egmond <[svanegmond@bang.dhs.org](mailto:svanegmond@bang.dhs.org)>

*Wed, 16 Aug 2000 21:47:07 -0400*

[http://www.ttc.ca/postings/gso-comrpt/documents/report/f910/\\_conv.htm](http://www.ttc.ca/postings/gso-comrpt/documents/report/f910/_conv.htm)

This URL gives an interesting report the Toronto Transit Commission describing an alarming situation on a revenue train. It provides a lot more detail than you might find in a media article.

The sequence of mechanical and human failures that contributed to the dangerous situation is interesting, as is the TTC's response, which includes:

- \* training (i.e., pounding on the table and saying "don't do that")
- \* reducing training (i.e., not teaching operators how to do a dangerous procedure)
- \* physical hacks

For background, the TTC runs trains in sets of six cars composed of three mated pairs. Each car has an operator's cab where motion and doors can be controlled, and a window which, when opened, reveals door control buttons.

Stephen van Egmond <http://bang.dhs.org/>

---

## **✶ Bangkok robot security guard**

Torrey Hoffman <torrey.hoffman@myrio.com>  
*Thu, 17 Aug 2000 09:49:24 -0700*

I think that even long-time RISKS readers will find this to be a bad idea of prize-winning magnitude. (Perhaps RISKS should give out yearly awards for

the worst (most risky) ideas implemented in software systems.  
Outlook VBS  
scripting comes to mind...)

The world's first armed robot security guard that can open fire on intruders while controlled through the Internet was unveiled in Bangkok yesterday. It is one of five Thai-made hi-tech robots revealed by the Thailand Research Fund.

Asst Prof Pitikhet Suraksa, of the King Mongkut Institute of Technology's Lat Krabang campus, said his roboguard was developed from an unarmed "telerobot" built in Australia in 1994. "The robot is equipped with a camera and sensors that track movement and heat. It is armed with a pistol that can be programmed to shoot automatically or wait for a fire order delivered with a password from anywhere through the Internet. With further development the technology could be applied to building robot guards for important places, including museums that house precious artifacts." [Was at [http://www.bangkokpost.net/170800/170800\\_News03.html](http://www.bangkokpost.net/170800/170800_News03.html)]

Deployment of this could lead to all sorts of interesting scenarios. The first time it perforates one of the cleaning staff, will the owners blame it on a "programming glitch"? [... potential puns about loose cannons ...]

Torrey Hoffman <Torrey.Hoffman@myrio.com>

[With no human in the loop, this would be really terrible. However, even with a human in the loop, it is another egregious example of

security

supposedly enforced by passwords floating sniffably unencrypted around the

Internet! And with a little IP spoofing, a penetrator might even be

untraceable. Perhaps Prof Suraksa needs an effrontal robotomy. As the

old joke goes, this may be a case in which you can always telerobot, but

you can't tell it much. PGN]

---

## ✈ Professor stole 40 student SSNs and IDs to get credit cards

"Pegasus" <pegasus@transport.com>

*Thu, 17 Aug 2000 17:19:05 -0700*

According to prosecutors, Cadello got names and Social Security numbers of

unwitting students from the school computer and named them as "parents" of

fictitious children whose Massachusetts birth certificates he forged. He

then obtained new Social Security numbers with those names and used them

to obtain various sets of ID and apply for credit cards (40 sets). The

incident has cost the university thousands of dollars for a new computer

system that lists students without using their Social Security numbers.

[[http://seattletimes.nwsources.com/news/local/html98/altprof17m\\_20000817.html](http://seattletimes.nwsources.com/news/local/html98/altprof17m_20000817.html)]

Central Washington professor sentenced in fraud, Mike Carter, \*Seattle

Times\*, 17 Aug 2000]

Here is the really weird part. When he was arrested the students protested

and gave him support (?). Well at least someone found a flaw in

their

database. Perhaps other colleges can learn from this one. ;-)

Joan L. Brewer BS CSE -- retired...

---

## ⚡ Kaiser Permanente medical e-mails go astray

Sheri Alpert <salpert@gmu.edu>

*Thu, 10 Aug 2000 02:18:59 -0400 (EDT)*

Beginning on 2 Aug 2000, Kaiser Permanente accidentally sent 858 e-mail

messages from nurses and pharmacists (some including sensitive medical

information) to the wrong people. Blame was placed on "human error" and a

"technological glitch" in upgrading their Web site. Kaiser spokesperson

Beverly Hayon said Kaiser has "fixed the problem. We have changed protocols

for sending out e-mails. We feel safe saying this particular problem will

never happen again." [Source: article by Bill Brubaker, \*The Washington

Post\*, 10 Aug 2000 E01]

---

## ⚡ Wake up, your TV is talking to your bracelet

"NewsScan" <newsscan@newsscan.com>

*Wed, 16 Aug 2000 09:51:39 -0700*

A new system called Whispercode, designed by a New Jersey company for

monitoring the effectiveness of TV advertising, will involve the encoding of

commercials with inaudible, identifying signals that can be

picked up by a small device worn by a participant (perhaps in a bracelet or keychain) and relayed to a nearby recording box that records the fact that the wearer was in the room when the commercial was broadcast. [It should be noted, though, the system can't detect whether the participant is awake, attentive, and not bored to death.] The company's chief executive officer says, "With Whispercode, we will finally be providing our clients with a true accounting of where their advertising money is going." (\*The New York Times\*, 15 Aug 2000 <http://partners.nytimes.com/library/financial/columns/081600tv-adcol.html>;  
NewsScan Daily, 16 August 2000

---

## **SSL Server Security Survey**

Monty Solomon <monty@roscom.com>  
*Sun, 13 Aug 2000 23:05:14 -0400*

SSL Server Security Survey, Eric Murray, ericm@lne.com 31 Jul 2000

A random sample of 8081 different secure Web servers running the SSL protocol in active use on the Internet shows that 32% are dangerously weak. These weak servers either support only the flawed SSL v2 protocol, use too-small key sizes ("40 bit" encryption), or have expired or self-signed certificates. Data exchanges with all types of weak servers are vulnerable to attack.

[http://www.meer.net/~ericm/papers/ssl\\_servers.html](http://www.meer.net/~ericm/papers/ssl_servers.html)

---

## **⚡ \*The Globe and Mail\* Web site exposing search-engine log file**

Esteban Gutierrez-Moguel <esteban@ce.net.mx>

*Thu, 17 Aug 2000 01:59:33 -0500 (CDT)*

The Web site of the Canadian newspaper \*The Globe and Mail\* seems to have a badly configured access policy of a log file. The log file is a standard Web server log file that contains browser information, requested data, and the IP address of each visitor who performs a search from the online edition of the newspaper.

A simple test of this problem is searching for some know text (for example: "Hello World") using <http://www.theglobeandmail.com> (Globe 7-day Search) and few seconds later you will find an entry in <http://archives.theglobeandmail.com/generated/Fragments/access> containing the string "Hello+World".

---

## **⚡ Blocked e-mail Web sites**

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

*Tue, 22 Aug 2000 12:14:06 PDT*

Lately, we have had another flurry of reports of perfectly reasonable Web sites and e-mail being blocked for the usual stupidities of overzealous filtering. But this one is somewhat different:

The U.S. Air Force Space Command blocked the San Francisco Exploratorium Yahoo site because it describes making a mixture out of baking soda and vinegar that would blow up a Ziploc bag. Elementary fizz-ics, my dear What's-on? [Source: [http://www.exploratorium.edu/pr/bubble\\_bomb.html](http://www.exploratorium.edu/pr/bubble_bomb.html)]

---

## ⚡ Major security hole in new online organizer service

Paul van Keep <paul@sumatra.nl>  
Wed, 16 Aug 2000 19:57:27 +0200

The recently opened online organizer service annapa.com (Anna, your Personal Assistant) suffered from a major security hole last week. The site has a security statement prominently displayed on its homepage with the usual statements about how they value their customers' data and that everything had been audited by Arthur Andersen.

Despite this, compromising other users' data was almost trivial: after logging in with the valid userid/password combo, all that had to be done was to twiddle with the URL which conveniently encodes your customer id. This simple operation gives access to all essential data from other users and allows changing of that data including blocking access by changing that user's password. The company behind annapa.com, IntraSites, issued a statement on its website in which it tried to belittle the issue. A

translation of the part of the statement currently on their homepage: "[...] updating some program modules on the site disabled one security mechanism. This made it possible for an IT-specialist (consequently not for a normal user), to access random and limited user data on the screen".

If all of that is true, what value does the security audit that AA performed have? Shouldn't AA review every update before installation? Is an IT-specialist not a 'normal' user? Aren't all crackers IT-specialists? Wouldn't a smart user be able to do the same? Was the hole only present for a couple of days? I sincerely doubt it.

The URL twiddling trick seems to be a common security problem. Two months ago I encountered almost the same hole in the customer information portal for Exact Software ([www.exactsoftware.com](http://www.exactsoftware.com)). The whole portal was removed from the site within an hour after I informed their CEO about the problem.

Paul van Keep <http://www.sumatra.nl>

---

## Hackers breach Firewall-1

"Peter G. Neumann" <[neumann@csl.sri.com](mailto:neumann@csl.sri.com)>

*Sun, 13 Aug 2000 19:52:47 PDT*

[Source: David Raikow, Sm@rt Partner, 2 Aug 2000

<http://www.zdnet.com/zdnn/stories/news/0,4586,2610719,00.html>]

An audience of several hundred network security professionals watched with

rapt attention last week as a trio of hackers repeatedly penetrated one of the industry's most trusted and popular firewall products -- Checkpoint Software's Firewall-1. The demonstration, presented at the "Black Hat" security conference in Las Vegas, challenged the widely accepted notion that firewalls are largely immune to direct attack.

The panel -- John McDonald and Thomas Lopatic of German security firm Data Protect GmbH and Dug Song of the University of Michigan -- identified three general categories of firewall attacks. They began by demonstrating a number of relatively simple techniques by which an attacker could impersonate an authorized administrator, and thus gain access to the firewall application itself.

A second type of attack tricked the firewall into believing an unauthorized Internet connection was actually an authorized virtual private network connection. Finally, the panel exploited a number of errors in the process used to examine traffic passing through the firewall to sneak in dangerous commands.

While their presentation focussed on a single commercial firewall product, panel members repeatedly emphasized that most firewalls are vulnerable to the types of attacks demonstrated. "The problem is not just with [Firewall-1]," said Song. "The real problem is the blind trust most people place in their firewalls."

Greg Smith, Checkpoint's director of product marketing for Firewall-1,

pointed out that many of the attacks demonstrated relied on improper firewall configuration, and he asserted that they presented little practical threat. "Not a single customer has reported a problem with any of these issues."

Nevertheless, Checkpoint worked with McDonald, Lopatic and Song in developing defenses against the attacks, which they released as part of Firewall-1 Service Pack 2 immediately following the demonstration.

Checkpoint emphasized that the service pack should prevent all of the attacks discussed, even those dependent on misconfiguration.

The panel also recommended a number of additional steps for "hardening" firewalls, including use of strong authentication protocols, "anti-spoofing" mechanisms and highly restrictive access rules. At the same time, they called on the IT community to abandon the "single firewall" model of network security and implement multiple lines of defense.

However, one observer of the session, employed by a network switch manufacturer, thinks Checkpoint lost some credibility over its products. "Some of the exploited areas were because of dumb programming mistakes in the code for the firewall itself. If the [firewall] programmers can't get it right, what other problems may still be lurking?" he pondered.

---

## **GAO says EPA's computer security is "riddled" with weaknesses**

Declan McCullagh <declan@well.com>

Sat, 12 Aug 2000 11:22:30 -0400

Exact URL is:

<http://com-notes.house.gov/ai00215.pdf>

Press release:

Bliley Releases GAO's Findings on Computer Security At EPA

Report Calls EPA's Computer Network "Riddled With Security Weaknesses"

Washington(August 11) --Ineffective, inadequate, and riddled with weaknesses.

This is how the General Accounting Office (GAO) described the Environmental Protection Agency's (EPA) agency-wide information security program.

Commerce Chairman Tom Bliley (R-VA), who in August 1999 requested the GAO audit of EPA's system as part of his review of the computer security policies and programs of certain Federal agencies within the Committee's jurisdiction, released the report today.

"The GAO report, coupled with the Committee's other recent oversight in this area, shows that, despite the tough rhetoric, the Clinton-Gore Administration's cyber-security policy amounts to little more than paper pushing," Bliley said today in releasing the GAO Report.

In February of this year, after GAO's preliminary review of EPA's system found "serious and pervasive problems," Chairman Bliley requested that EPA take down its computer systems and initiate a major overhaul of its computer network security. The EPA reluctantly complied.

"It is unfortunate," Bliley said, "that years of gross mismanagement at the Agency have left these sensitive systems and data at such serious risk for so long. But it is even more unfortunate that it took this Committee's oversight and public pressure to motivate the Agency to undertake responsible steps to ensure its computer systems provide adequate protection for sensitive Agency data.

"EPA, while shocking in degree, is not alone when it comes to poor management of cyber security. GAO and Committee oversight of other Federal agencies continues to reveal that, rather than being a model for the private sector to follow -- as the President has claimed he wants it to be -- the Federal government appears instead to be a model of what not to do when it comes to managing information security.

"In today's world, information security is crucial. It is disturbing that government agencies with critical computer systems have paid so little attention to this issue, and are so vulnerable to attacks. It also reflects a lack of leadership from the White House, which under current law should be coordinating agency efforts to improve cyber security, but isn't.

"I will continue my review of agency information systems in an effort to improve the Federal government's weak computer security practices."

In late July 2000, Bliley requested the GAO complete a similar audit of the Commerce Department's cyber security program. Bliley also recently launched

a review of the Food and Drug Administration's (FDA) information management policies and practices, requesting records detailing the agency's computer security practices and any hacker attacks against FDA.

a copy of the GAO Report is available at: [www.house.gov/commerce](http://www.house.gov/commerce)

---

## ✶ Bruce Schneier's Secrets and Lies

"Peter G. Neumann" <[neumann@csl.sri.com](mailto:neumann@csl.sri.com)>

*Tue, 22 Aug 2000 12:14:06 PDT*

Bruce's new book, *\*Secrets and Lies: Digital Security in a Networked World\**

(Wiley), concludes that cryptography alone cannot protect business networks.

This a fine counterpoint to the mistaken belief that cryptography is the ultimate answer to security.

"Protecting information has become increasingly difficult in the digital world. Teen-aged hackers have compromised the security of the U.S. State

Department's web site and, in so doing, have proven that gaining access to

personal passwords and other `secure' information is far easier than many could have ever anticipated."

The book website is

<http://www.counterpane.com/sandl.html>

and is discussed in

<http://www.counterpane.com/crypto-gram-0008.html#1>

---

## Software Risk Management Conference ISACC

Gary McGraw <gem@rstcorp.com>

*Fri, 18 Aug 2000 14:09:13 -0400*

Reliable Software Technologies encourages all people interested in making software behave to attend ISACC, the Software Risk Management conference

(<http://www.isacc.com>). We'll be discussing many of the topics RISKS

readers are fond of: security, reliability, and safety. And just to spice

things up, how about software certification as a controversial issue?! Hope

to see you there.

Gary McGraw, Ph.D      gem@rstcorp.com, Vice President, Corporate Technology

Reliable Software Technologies, Dulles, VA <<http://www.rstcorp.com/~gem>>



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 21: Issue 3**

**Monday 28 August 2000**

## Contents

- [New security vulnerability: 13-year-old 'r00ts' popular polynomial](#)  
[Leonard Richardson](#)
- [Pretty Good Bug found in Windows versions of PGP](#)  
[Declan McCullagh](#)
- [Two cables](#)  
[Doneel Edelson](#)
- [Four of the 13 root servers used by Network Solutions](#)  
[Dave Farber](#)
- [Court says FBI has been given too much wiretap power](#)  
[NewsScan](#)
- ["Free" e-mail accounts and passwords exposed for a month](#)  
[Peter Kaiser](#)
- [Hotmail blows it badly?](#)  
[Jay R. Ashworth](#)
- [Possible Y2K bug strikes UK Egg Bank](#)  
[Ralph Corderoy](#)
- [More risks of filtering software](#)  
[David Goddard](#)
- [Risks of Eurdora 4.x](#)  
[David Sedlock](#)

- ["Verify your age with a credit card": more than \\$188M fraud](#)  
[Lenny Foner](#)
  - [Re: Airline E-tickets](#)  
[Adam Shostack](#)
  - [Re: Hoaxes: when will they ever learn](#)  
[Eric Murray](#)
  - [Re: SSL Server Security Survey](#)  
[Sean Eric Fagan](#)
  - [Re: mechanical and human failures in Toronto](#)  
[Mark Brader](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

## ⚡ New security vulnerability: 13-year-old 'r00ts' popular polynomial

Leonard Richardson <leonardr@segfault.org>

Thu, 24 Aug 2000 13:59:24 -0500

[With permission, at the request of PGN.]

### 13-Year-Old 'r00ts' Popular Polynomial

The well-known polynomial  $x^2+8x+6$  was defaced today by a teenager who had "r00ted" the beloved function of one variable through the use of a popular script known as "QuAd 3QaZh0n". The attack set off the usual sequence of events: an initial panic setting off an orgy of media hype reaching a crescendo with an article in the mainstream media, a string of copycat successors, and a meaningless stream of empty promises from vendors who immediately lapsed back into apathy as the incident left the public's short-term memory.

Segfault spoke with the culprit, who goes by the name of "2o31js34g", although his real name is Alvin Schumaker. "I did it for the kicks," said the eighth-grade desperado. "Also, it was problem 12 on my algebra homework."

Schumaker's admission that he had learned the technique used to crack the equation "in class" led to sweeping reforms at Nathan Hale Middle School, his alma mater. These range from a draconian school uniform policy to periodic cavity searches to Internet filters on library computers so restrictive that they ban the school's own home page.

"If these kids would just study their math, we wouldn't have anybody learning these dangerous equation things," said Nathan Hale principal Fred Fractal, previously known for shutting down the wood shop because "those nail things look like weapons."

Numerous other tools are available for cracking polynomials exist, such as Fac-t0R. More worrying are tools for "solving" large groups of linear equations at a time; one such program makes reference to a "matrix", obviously an homage to the sci-fi classic.

Many such programs are distributed for the TI series of "calculators", tools widely viewed as a security threat in many fields and rings. Disturbingly, such devices are increasingly being made available to high school and college students. Public policy must now answer the question: where is the line to be drawn between useful tool and bloodthirsty weapon

of mathematical carnage? Who will answer for the countless linear equations to have undergone Gaussian elimination?

Predictably, immediately following the defacement, thousands of polynomial security companies came out of the woodwork to hawk their shoddy products.

"Our proprietary polynomials are one hundred percent safe because they have no roots at all," said Len Eir of Rootless.com, a company offering sales and consulting for polynomials such as  $x^2+4$  and  $x^6+x^2+101$ . Despite Eir's claims, attacks on such polynomials are not uncommon, although Eir dismissed all such reports as "imaginary".

Dave Errential of Integrated Systems stated: "Integration technology makes it easy to add roots to your polynomial. Take  $60x^2+264x$ , for instance. The roots for that polynomial have been posted in a million places on the web. But our proprietary integration technology can turn that into  $5x^4+44x^3$ ! I'd like to see someone try and find the roots of that polynomial!" [Try  $x=0$ . --Ed.] Research has shown that IS polynomials are vulnerable to several types of attacks, but, again, the vendor has chosen to go after the research, calling it "derivative", rather than investigate the vulnerabilities.

"Our polynomials are of a magnitude so high that it would be impossible to find their roots even with the most sophisticated technology," said OrderOfMagnitude.com's Sean Gular. "Our proprietary technology allows us to offer  $x$  to the power of one billion,  $x$  to the power of one

trillion, even x  
to the power of ten gazillion! No one can crack these  
polynomials!" [Try  
x=0. --Ed.]

"It's irresponsible to distribute these polynomial-cracking  
kits," says  
security expert Bruce Schneier of Counterpane Internet  
Security. "It's like  
teaching a baby how to do surface integrals. He doesn't  
understand the  
socially responsible way to use this knowledge, so he wreaks  
havoc." For  
improved security, Schneier urges all polynomials to be of  
fourth order or  
higher, and to change roots at least once every two weeks.

Originally published on segfault.org:

<http://segfault.org/story.phtml?id=396f3e5c-0958dfa0>

Written by Leonard Richardson <leonardr@segfault.org>

Posted on Fri 14 Jul 09:24:53 2000 PDT

[Bastille Day, eh? Well, although it is a little late for the  
1 April

RISKS issue, this item seemed very timely in light of certain  
continuing

efforts to control the underpinnings of cryptography. PGN]

---

## **🔥 Pretty Good Bug found in Windows versions of PGP**

Declan McCullagh <declan@well.com>

*Fri, 25 Aug 2000 08:19:40 -0700*

Background:

<http://www.politechbot.com/p-00067.html>

<http://cgi.pathfinder.com/time/digital/daily/0,2822,12854,00.html>

<http://www.wired.com/news/print/0,1294,16219,00.html>

FC: Pretty Good Bug Found in PGP, by Declan McCullagh

(declan@wired.com)

25 Aug 2000

A bug in newer versions of Network Associates' popular PGP software exposes purportedly scrambled communications to prying eyes.

Network Associates (NETA) Thursday confirmed the vulnerability, discovered by a German cryptanalyst, which allows malicious attackers to hoodwink Windows versions of PGP into not encoding secret information properly.

The bug appeared in controversial features that the company included to satisfy government and corporate demands for key recovery, a technology that allows a third party to read encrypted communications. [...]

In December 1996, the company that became Network Associates joined the Key Recovery Alliance, a group of dozens of companies trying to promote the idea of key recovery and key escrow technologies. Federal government regulations at the time gave preferential treatment to such products.

Because of PGP's long history of institutional opposition to key recovery, Network Associates dropped out after buying the smaller software company. But in February 1998 they purchased Trusted Information Systems, a founder of the Key Recovery Alliance.

"Trusted Information Systems has been a pioneer in key recovery and the Key Recovery Alliance where over 60 companies and systems vendors like IBM, Hewlett-Packard, Sun Microsystems, Boeing and Motorola are supporting their key escrow capability that allows for the export of strong encryption under

U.S. Commerce laws," Network Associates CEO Bill Larson said in an interview on CNNfn at the time.

Months later, Network Associates had quietly rejoined the Key Recovery Alliance. [...]

---

## ⚡ Two cables

"Doneel Edelson" <doneel.edelson@eulergroup.com>

*Mon, 28 Aug 2000 12:28:53 -0400*

During the Verizon strike, two New York employees attempted to cut a telephone cable with wire shears. Two cables were running up the side of a pole, one was for telephone service and the other was a high-voltage electric line serving about 4000 homes. They cut the wrong cable, showering hot sparks that burned their clothes and skin. The main part of the voltage ran up the pole; however, the heat was enough to melt the blades of the wire shears. The two were caught by the police, arrested, and treated at a local hospital.

[Treated to what? Quite a trick. (It's too early for Hallowe'en.)

I guess in this context "Pride in your work" becomes "Fried in your shirk" (with multiple meanings and a pun).  
Strike while the irony is hot? PGN]

---

## ⚡ Four of the 13 root servers used by Network Solutions (From

## IP)

Dave Farber <farber@cis.upenn.edu>

*Fri, 25 Aug 2000 18:02:53 -0400*

Four of the 13 root servers used by Network Solutions to manage global Internet traffic partially failed for a brief period Wednesday night due to technical difficulties. The computers -- one in Tokyo, one in California and two in Virginia -- failed to serve requests for links to Web sites ending in ".com" suffix for a little over an hour. Web addresses ending in other suffixes were unaffected. While an e-mail distributed Wednesday by Network Solutions VP Mark Rippe described the event as "a \*MAJOR, MAJOR\* incident", an NSI spokesman later insisted the failure was simply "a minor hiccup invisible to end users." Minor hiccup indeed. The last time something like this happened, July of 1997, it was seven root servers that failed, disrupting much of the traffic on the Net for a few hours.

["End user" is an interesting term in this context. Users were left

with ends that were not connected. If the ends justify the means,

then I suppose we need to have "mean" users as well. As in the movie

\*Network\*, we need to at least get mad, if not mean. I mean it. PGN]

---

**⚡ Court says FBI has been given too much wiretap power**

"NewsScan" <newsscan@newsscan.com>

Wed, 16 Aug 2000 09:51:39 -0700

A three-judge panel of the U.S. Court of Appeals for the District of Columbia has ruled that the Federal Communication Commission's attempts to implement a 1994 electronic wiretap law have been too accommodating to law enforcement agencies and not sufficiently protective of the right of citizens to individual privacy or of the financial requirements of companies. The wiretap law (the Communications Assistance for Law Enforcement, or CALEA) was passed by Congress because the FBI had insisted it was losing ground against criminals because wireless phone companies were not designing wiretapping capabilities into their networks. An executive of the Center for Democracy and Technology, which had opposed the FBI's request to Congress, says the appellate court's decision means that "government cannot get its hands on what it's not authorized to get just by promising it won't read what it's not supposed to read." [\*The Washington Post\*, 16 Aug 2000; NewsScan Daily, 16 August 2000; <http://www.washingtonpost.com/wp-dyn/articles/A32193-2000Aug15.html>]

---

## ✶ "Free" e-mail accounts and passwords exposed for a month

Peter Kaiser <kaiser@acm.org>

Thu, 03 Aug 2000 23:19:54 +0200

Zurich newspapers have just reported a horrible security lapse at one of

Switzerland's big Internet service providers, Sunrise. Sunrise is the second biggest telecommunications provider in Switzerland, and like the two other big telephone providers -- Swisscom and diAx -- also offers Internet service.

From July 2 to August 1, following a hardware upgrade, a search page supposed to be used only internally by Sunrise was exposed to external use, allowing anyone to look up e-mail account names and passwords. Sunrise knows that these data were accessed from at least twenty different locations to collect data on at least 700 (of about 300,000) accounts. Sunrise has sent e-mail to all its ISP customers advising them to change their passwords. The national data protection officer, Odilo Guntern, is reported as saying that the security lapse is a clear breach of the rules concerning protection of such data, and that he will be discussing it with Sunrise.

Although it's not stated clearly, the tenor of the articles seems to be that the passwords were stored unencrypted. This reaches a too-familiar depth of careless design, especially coupled to their not noticing the situation for a month. It appears that the ability to do these searches was always there, protected only through the tiny obscurity of not making the search page externally accessible; but actual searches required no authentication. Perhaps they still don't.

But that's not the only evidence of poor judgment; they've been

clueless

from the beginning. As a Sunrise phone customer I was among the first to get their offer of "free" Internet service, and of course I took a look.

The signup page asked for an account name and password, but was unsecured.

Not only did I abandon immediately the idea of signing up with them, but I

called the next day and tried to get through to whomever was responsible

for that particular stupidity; and although I talked to a lot of people,

not one of them seemed to understand the risk of transmitting account

information unencrypted. The least clueless of them told me that in any

event it was software bought from a third party, and they had no control

over it. I eventually gave up.

Recently Sunrise began offering its phone customers another "free" service,

storage and forwarding for voice messages and faxes, with signup over the

web or via their call center. I went to the signup page and damn if it

wasn't ANOTHER request for a password via an unsecured form page! I want

to use the service, so I phoned the call center, which set it up at once

over the phone. Once again I brought up the risk of doing it unsecured

over the net, and the young lady at the call center told me "We prefer

people to do it by telephone anyway, because it's easier for us."

Many RISKS and obvious errors here, none of them new.

[I have probably said it before here: ALWAYS look a Trojan horse in the

mouth, whether it is free or not. PGN]

## ✂ Hotmail blows it badly?

"Jay R. Ashworth" <jra@baylink.com>

*Fri, 25 Aug 2000 13:31:44 -0400*

Members of the RISKS community are well aware of the problems that can happen when one user impersonates another on purpose. We've also seen porn purveyors cruise in behind the producers of less... exciting movies, and grab their expired top level domain names -- names which should never have been registered at the top level in the first place, because they were, by design, disposable.

Well, there's a new contender in that category.

Hotmail.

According to this story

<[http://www.computerworld.com/cwi/story/0,1199,NAV47\\_ST048970,00.html](http://www.computerworld.com/cwi/story/0,1199,NAV47_ST048970,00.html)> ,

Hotmail is having a problem with buddy lists:

- > Microsoft is investigating a complaint that expired Hotmail accounts
- > retain the linked MS Instant Messenger buddy lists, and those lists
- > are available to the next person who registers the same e-mail address
- > on a Hotmail account.

That's all fine and dandy, but it was the last clause that worried

\*me\*: "registers the same e-mail address".

What? You *can* do that? They *allow* the reuse of names?

There are so many possible risks there that I don't think I  
\*can\* enumerate  
them. Even \*AOL\* has this right: once a screen name has been  
dropped, it's  
no longer reusable.

Not that I ever thought Hotmail was a great idea in the first  
place, now I  
have even more reason to tell people not to use it. I wonder if  
they've  
finally gotten it to run on NT? :-)

Jay R. Ashworth <jra@baylink.com>, The Suncoast Freenet, Tampa  
Bay, Florida  
<http://baylink.pitas.com> +1 727 804 5015

---

## **⚡ Possible Y2K bug strikes UK Egg Bank**

Ralph Corderoy <ralph@inputplus.demon.co.uk>  
*Wed, 23 Aug 2000 22:52:08 +0100*

I've just received my first statement for an account with the  
UK's Egg  
Bank; [www.egg.com](http://www.egg.com). It was triggered by the annual interest  
payment on  
the 19th August 2000. The account has been opened for just  
under a  
year. The statement goes something like this.

Opening balance.		0.00
19 Aug 1999	Interest gross	xx.xx
19 Aug 1999	Tax deduction	-xx.xx
23 Aug 1999	Deposit	xx.xx
15 Oct 1999	Deposit	xx.xx

According to the above statement, the interest was paid before  
any money was  
in the account. If I inspect the account online the two  
interest entries

are at the bottom of the statement dated correctly 19 Aug 2000.  
When telephoning Egg's service staff they also viewed the account on their computers with the correct year 2000 date. They seemed unconcerned that the printed statements they were sending people had the wrong year since the amount of interest was correct anyway. I doubt my report has been passed on internally by them.

It's interesting to see what might be a Y2K bug popping up eight months after 1st Jan 2000 in an `Internet' bank that has only been running a year or two.

Since information regarding interest received and tax paid has to be passed onto the Inland Revenue (the UK's IRS) as part of an individual tax return for the year this could cause problems for individuals when they fail to produce supporting material with the dates they are claiming.

[Egg on the face of it? PGN]

---

## **✶ More risks of filtering software**

"David Goddard" <David.Goddard@cognos.com>  
*Mon, 28 Aug 2000 12:08:47 -0400*

The subject of usernames containing "offensive" words being automatically banned from blackplanet.com has recently received some publicity on Declan McCullagh's Politech list, with the filtering software getting upset about the name 'Babco\*k'. Interestingly, the filtering software at

blackplanet.com could be criticised not for what it doesn't let through but what it does -- it appears to accept usernames based around the British swear words 'ar\*e' and 'wa\*k', for example. [PGN-ed asterisks just to avoid blocking of this issue?] It's a sure bet that many obscenities in other languages can also be used. Given that blackplanet.com appears to be aimed at a partly international audience, this is pretty poor.

The RISK, yet again, is the blind faith in a software solution that a) operates only with a limited scope and b) returns false positives which irritate users and ultimately generate bad publicity. Given the many creative ways of coming up with offensive usernames and the obvious problems with being too restrictive, maybe they would be better off just relying on robust Terms Of Service and maybe a little grepping of the user lists.

[I wonder in what language "grep" is a bad word! Grep Suzette? PGN]

---

## Risks of Eudora 4.x

"David Sedlock" <david.sedlock@step.de>  
*Mon, 28 Aug 2000 09:04:34 +0200*

I have used the "lite" version of Eudora for some time. It was good enough for my undemanding needs I recently upgraded to the latest Eudora, which doesn't provide a separate lite version, but instead offers three modes:

full-featured paid, full-featured free paid by ads, and limited-feature free with no ads. The second mode fetches ads from the Eurdora site via HTTP.

The differences in the modes were clearly explained and after firing up the program I soon decided the limited-feature free mode with no ads was good enough for me. After choosing that and restarting the program the entries in my proxy log for the Eurdora site appeared to stop and I thought that was the end of the matter.

However, looking in the proxy log a few days later to solve an unrelated problem, I was perplexed to find new connections to the Eudora site. In fact, the mail tool was connecting to a Java servlet in a directory called "adserver" about twice a day.

I wrote to both the webmaster and customer service (as a nonpaying user you don't even get a support e-mail address) and heard nothing for a few days. I wrote back and threatened to go public and then got two answers. One came from a technical person who said Eudora is checking for upgrades and I can turn this off by adding a few lines in its ini file. I did and the connections didn't stop. The other came from a non-technical person who said the connections were there to support "co-branding" (whatever that is) and not to worry since they happen "really really fast" and don't divulge "any private data". This reply failed to comfort me, since after all I pay for the price of a phone call to my provider if I'm not hooked up when Eudora

decides to co-brand and my dialing daemon fires up. I wrote again for clarification and have yet to receive a reply.

The risks? Many come to mind, but the one that stands out is software that silently carries out unexpected actions. One day our PCs may be so bound up with the Internet that we expect a software program to make unannounced connections to external servers, but today I don't expect that a mail client has any need to connect to external servers except when it is sending or receiving mail. Today such connections need to be documented and announced. Eudora was clear about its fetching ads in the "full-featured free paid by ads" mode, and I have no problem with that. But the fact that after choosing the limited-feature mode the program continued connecting was totally unexplained and probably goes on undetected by the majority of users.

Eudora, you're in the dog house!

David Sedlock

---

## 🔥 "Verify your age with a credit card": more than \$188M fraud

Lenny Foner <foner@media.mit.edu>

*Fri, 25 Aug 2000 14:29:33 -0400 (EDT)*

Back when the CDA was hot news, lots of people were claiming that "asking for credit card numbers" was a reasonable way to prove that someone was "old enough" to view certain web sites. Below is a great example---one which

people have been warning about for years---of why this is a horrendous idea, even if you don't care about the civil liberties implications [see [\*] below] of using a credit card as an age check, or of having an age check at all:

#### U.S. CRACKS DOWN ON NET PORN FRAUD

The Federal Trade Commission has filed a lawsuit against Crescent

Publishing Group and 64 affiliated companies that operate adult Web sites, accusing them of charging customers for services advertised as "Free Tour

Web Sites." Like many adult sites, the Crescent sites requested that users

supply credit card information to verify they were of legal age to view

pornographic material. Customers who'd been promised a free online peep

show say they were then billed for recurring monthly membership fees

ranging from \$20 to \$90. Included among the complainants were some people

who said they'd never visited the sites at all -- in fact, one woman who'd

been charged a recurring fee for several months didn't even own a computer.

To add to the confusion, the charges were made under different company

names. Instead of finding a charge from Highsociety.com on their

statements, consumers would find charges from "Online Forum," or "Hoot

Owl," or "Knock Knee." The FTC has classified the scam as one of the

largest it's ever seen on the Internet, generating \$141 [million]

in the first 10 months of 1999 alone. (E-Commerce Times 24 Aug 2000)

<http://www.ecommercetimes.com/news/articles2000/000824-4.shtml>

(The above was from NewsScan; the full story is at the cited URL, including how the company moved to Guatemala to continue the scam.)

[\*] What civil liberties problems? How about:

(a) It discriminates against people who are too poor or have too bad

a credit history to own a card (including those who've gone bankrupt)

(b) It identifies people to sites in a very accurate and intrusive

way, by name, rather than simply making it clear that they are

"old enough". Remember, it's age, not identity, that such sites

are supposed to be caring about.

(c) "Old enough" varies based on where you are, even in the US and

especially in the world, but this system makes no provisions for that.

(d) How old you have to be to get a credit card varies by country,

and many countries don't have the sort of credit-card presence

that the US does, which might make it impossible to get one at

all.

(e) It assumes that differentiating content by age is a reasonable

idea in the first place.

These are just the most obvious ones off the top of my head.

I'm sure

these, and more, were all mentioned prominently at the time.

But, of

course, the bad system of credit-card verification took hold anyway, and we

seem to be stuck with it.

[Also, from a purely security standpoint and not a civil-liberties

standpoint, this also assumes that no kid is going to be bright enough to copy down a parent's CC info while they're not looking. Surely all parents ensure that all their credit cards are secured 24x7. Of course, they can't use a -key-, unless that key is also secured and/or on their person 24x7...  
Wait---parents don't tend do this?]

---

## **⚡ Re: Airline E-tickets (Wallich, [RISKS-21.02](#))**

Adam Shostack <adam@zeroknowledge.com>

*Sun, 27 Aug 2000 13:03:03 -0400*

> swipe a credit card or other means of ID [...]

I have two comments here. The first, as the credit card companies will tell you, their cards are not meant to be used as identification (just like the social security card.) [And yet, they are! PGN]

The second is it seems likely [...] that someone willing to go to the trouble of blowing up an airplane can't be bothered to engage in a little identity theft or ID-card forgery.

Adam

[Similar comments from Ian Lance Taylor, Marc Auslander, Jim Rees... PGN]

---

## **⚡ Re: Hoaxes: when will they ever learn**

Eric Murray <ericm@lne.com>

*Sun, 27 Aug 2000 09:46:13 -0700*

A digital signature on the press release would not have prevented this -- it was a real press release sent out by Internet Wire, a business press-release agency.

The hoaxers got the release sent by social-engineering IW- they convinced a "day staff" that the "night staff" had approved the story. [Source: (San Jose) \*Mercury News\*, 26 Aug 2000]. Thus the story was accepted without checking the facts.

The real problem here is shoddy "journalism". Digital signatures would have prevented this only if IW accepted only e-mailed releases that were digitally signed, and they actually verified the signatures. If they accepted phoned-in releases, hoaxers could still send in fakes ones. Fixing the verification procedure is the way to prevent this sort of problem from occurring again.

Eric Murray <http://www.lne.com/ericm> ericm at lne.com  
Consulting Security Architect

---

## **✶ Re: SSL Server Security Survey (Solomon, [RISKS-21.02](#))**

Sean Eric Fagan <sef@kithrup.com>

*Sun, 27 Aug 2000 03:46:04 GMT*

Self-signed certificates are *\*not\** any weaker than those signed by

third-party certificates. This is a popular myth I keep running into -- all a third-party-signed certificate means is that someone else has agreed that you are who you say you are. And in the case of Web browsers, it also means that this someone forked out a load of cash to Microsoft and/or Netscape to be included in the default set of known certificates.

---

## **⚡ Re: mechanical and human failures in Toronto (van Egmond, [Risks-21.02](#))**

Mark Brader <msb@vex.net>

*27 Aug 2000 04:06:46 GMT*

> Each car has an operator's cab where motion and doors can be controlled,  
> and a window which, when opened, reveals door control buttons.

I think the last sentence is misleading enough to merit correction. There are indeed door control buttons outside of the cabs: as the cab is only on one side of the train, this allow the doors on the other side to be opened without the guard having to cross to the next car. But exposing these buttons requires a key, presumably the same one that opens the cab.



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 21: Issue 4**

**Monday 11 September 2000**

## Contents

- [Identity theft](#)  
[PGN](#)
- [Government computers at risk](#)  
[NewsScan](#)
- [Satellite system outage hits Associated Press](#)  
[Keith A Rhodes](#)
- [Puerto Rican capital without power](#)  
[Doneel Edelson](#)
- [New Pentium III chip recalled](#)  
[NewsScan](#)
- [CSX crew spots problem signal, averts collision](#)  
[Chuck Weinstock](#)
- [F-117 stealth fighter in near-miss with UAL jet](#)  
[PGN](#)
- [Fake air controllers alert in UK](#)  
[Joe McCauley](#)
- [Swissair 111, TWA 800, and Electromagnetic Interference](#)  
[Fred Ballard](#)
- [D.01: off by x100 stock prices](#)  
[Bob Blakley](#)

- [Western Union Web site hacked](#)  
[Keith A Rhodes](#)
  - [FBI arrests Emulex hoax suspect in Calif.](#)  
[NewsScan](#)
  - [Glitch at Amazon.com exposes e-mail addresses](#)  
[Keith A Rhodes](#)
  - [Windows NT/2000 "Lock Computer" allows palm sync](#)  
[Avi Rubin](#)
  - [1,000 system updates???](#)  
[Scott Rainey](#)
  - [Risks of partially updated Web pages](#)  
[Daniel P.B. Smith](#)
  - [Re: Major security hole ...](#)  
[Chris Adams](#)  
[Michael Loftis](#)
  - [Re: Your TV is talking to your bracelet](#)  
[George Weaver](#)
  - [PFIR statement on government interception of Internet data](#)  
[Lauren Weinstein](#)
  - [REVIEW: "Big Book of IPsec RFCs", Pete Loshin](#)  
[Rob Slade](#)
  - [2001 IEEE Security and Privacy Symposium](#)  
[Jon Millen](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

## ⚡ Identity theft

"Peter G. Neumann" <neumann@csl.sri.com>  
*Mon, 28 Aug 2000 15:14:49 PDT*

A news brief in the California Public Interest Research Group (CALPIRG) Citizen Agenda, Summer 2000, p.6, is worth noting here, with the rapid increase in identity theft. We used to see a case or two a

year. Now they seem to be coming in much more often, perhaps a few each month.

### Survey Details Hassles of Identity Theft

Identity theft victims spend two years or more removing an average of

\$18,000 in fraudulent charges from their credit reports.

''Unless

new laws force banks, department stores and credit bureaus to clean up

the identity theft mess, this crime is only going to get worse.''

said CALPIRG's Dan Jacobson -- who is urging state lawmakers to back proposals

pending in the Legislature that would allow consumers to block access to

their credit reports and streamline law enforcement investigation and

victim assistance programs.

Try sending e-mail to [calpirg@pirg.org](mailto:calpirg@pirg.org) to request the report.

Unfortunately

their Web site at [www.calpirg.org](http://www.calpirg.org) is apparently still under construction

as I write this.

---

## **Government computers at risk**

"NewsScan" <[newsscan@newsscan.com](mailto:newsscan@newsscan.com)>

*Mon, 11 Sep 2000 08:33:37 -0700*

A new study released by the General Accounting Office has exposed widespread

deficiencies in computer security in government agencies ranging from the

Department of Interior to the U.S. Treasury. The report comes nine months

after the President Clinton called on federal agencies to beef up security in his "National Plan for Information System Protection." That plan proposed that Congress boost federal spending for computer security and research by \$280 million to \$2.3 billion in 2001, but agencies say they need the money now. Government computer managers point to the tight labor market for computer security experts and say it's difficult to retain good personnel. The GAO report found that some agencies have failed to take even the most rudimentary steps to increase security, such as encrypting password files and limiting physical access to sensitive computers. In addition, agencies have been less than diligent about blocking access for independent contractors and former employees after they've left the government. In one agency, 7,500 of 30,000 users were not deleted after 160 days of inactivity. "The federal government, outside the defense area, is worse than the private industry because good computer security is about regular maintenance and housekeeping -- and that's not one of the government's strong points," says Stewart Baker, a Washington, D.C. technology lawyer. (Los Angeles Times 11 Sep 2000; NewsScan Daily, 11 Sep 2000  
<http://www.latimes.com/business/20000911/t000085464.html>)

---

## **✶ Satellite system outage hits Associated Press**

"Keith A Rhodes" <rhodesk.aimd@gao.gov>  
*Thu, 31 Aug 2000 07:25:30 -0400*

The Associated Press reported on 29 Aug 2000 that a satellite system outage disrupted AP services providing radio and TV stations with certain specialized info, as well as some smaller newspapers that receive AP Basic, beginning around 5:15 a.m. after new software was downloaded to satellite receivers on AP's Ku-band system. Partial service was restored that afternoon, but full service was estimated at taking several days. [PGN-ed]

---

## **✶ Puerto Rican capital without power**

"Edelson, Doneel" <doneel.edelson@eulergroup.com>

*Thu, 7 Sep 2000 11:11:35 -0400*

A break in a 231,000-volt line carrying power over the mountains left the Puerto Rican capital of San Juan without power Thursday morning, trapping dozens of people in elevators, slowing rush-hour traffic when traffic lights failed, knocking out air conditioning, and forcing many businesses to close. About 500,000 customers were affected for most of the day. A helicopter crew was sent out to do the repair. [Source: AP item, 7 Sep 2000; PGN-ed]

Doneel Edelson, Information Technology, EULER American Credit Indemnity

1-410-554-0797 doneel.edelson@eulergroup.com

---

## **⚡ New Pentium III chip recalled**

"NewsScan" <newsscan@newsscan.com>

*Tue, 29 Aug 2000 09:45:34 -0700*

Intel is recalling its 1.3 gigahertz Pentium III chip, which it has sold to only "a handful" of "power users" running advanced applications, because a certain combination of data, voltage, and temperature conditions may cause the chip to fail. The chip is expected to be back on the market in a couple of months. (Reuters/\*The Washington Post\*, 29 Aug 2000 <http://www.washingtonpost.com/wp-dyn/articles/A40772-2000Aug29.html> NewsScan Daily, 29 August 2000)

---

## **⚡ CSX crew spots problem signal, averts collision**

Chuck Weinstock <weinstock@sei.cmu.edu>

*Tue, 29 Aug 2000 23:14:26 -0400*

An alert CSX crew (in Fredericksburg VA) noticed an erroneous proceed-signal indication on a parallel track on 8 Aug 2000. By contacting the dispatchers (in Jacksonville FL), they prevented a collision between Amtrak's Auto Train and a Virginia Railway Express commuter train. The incident prompted the inspection of the insulation of a certain type of old (TC Green, 1948 to 1962) signal wiring that may be still in use in thousands of signals nationwide. [Source: \*Trains Magazine\*, <http://www.trains.com>,

commenting

on an article by Don Phillips in \*The Washington Post\*, 17 Aug 2000; PGN-ed]

---

## **✈ F-117 stealth fighter in near-miss with UAL jet**

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

*Mon, 11 Sep 2000 08:13:11 PDT*

An F-117 on a training flight on 7 Sep 2000 flew quite close to United Airlines flight 174 from LAX to Boston. The UAL's TCAS system apparently detected the incoming fighter (the fighter was broadcasting its position), and triggered a scramble to avoid a possible collision. This opens up a lot of questions, such as why was the stealth flying at 500 feet vertical separation from the UAL flight at 10,800 feet (and .6 mile horizontal when detected), in the LAX take-off corridor? Was the fighter under proper air-traffic control? There have been enough Air Force incidents lately that more caution would seem to be in order. Besides, there is always the risk with TCAS that both planes try responsive maneuvers that make things worse -- especially at high closing speeds, perhaps something less than 5 seconds in this case. Preliminary reports seem to indicate controller error, which is not surprising given the ever increasing stresses on an already stressed and archaic operational environment.

## **✶ Fake air controllers alert in UK**

Joe McCauley <mccauley@davesworld.net>

*Tue, 29 Aug 2000 10:22:16 -0500*

Britain's Civil Aviation Authority has noted various cases in which "radio hackers" have commandeered air-traffic control communications, giving false instructions or fake distress calls. The number has risen from 3 in 1988 to 18 in 1999, and 20 thus far in 2000. A case at Washington's Reagan International in April 1999 was also noted. [RISKS has reported a few such cases years ago, including a Miami masquerader, the Roanoake Phantom -- and the Manchester (UK) spoofer in 1996.]

[http://dailynews.yahoo.com/h/ap/20000827/wl/britain\\_fake\\_air\\_controllers\\_1.html](http://dailynews.yahoo.com/h/ap/20000827/wl/britain_fake_air_controllers_1.html)

<http://abcnews.go.com/sections/us/DailyNews/FakeAirTraffic000829.html>

Joe McCauley [contributed by others as well. PGN]

---

## **✶ Swissair 111, TWA 800, and Electromagnetic Interference**

Fred Ballard <fred.e.ballard@abbott.com>

*Wed, 6 Sep 2000 13:22:13 -0500*

Until I read Elaine Scarry's "Swissair 111, TWA 800, and Electromagnetic Interference" in the September 26, 2000 issue of the New York Review of Books

at <http://www.nybooks.com/nyrev/WWWfeatdisplay.cgi?20000921092F>,  
I had no  
idea that both flights took off from JFK airport at 8:19 p.m. on  
a Wednesday  
night, but that's only the beginning. It seems the role of  
electromagnetic  
interference in the downing of both flights has yet to be fully  
explored.

Of particular interest to RISKS readers is that Swissair 111 may  
have been  
unable to detect a problem until it was too late because of the  
plane's  
ability to reconfigure its electrical systems in the event of  
problems:

Swissair 111 was an MD-11, a type of plane made by  
McDonnell-Douglas  
and derived from the DC-10. When the MD-11 first appeared  
in the 1990s,  
its "design philosophy" was widely celebrated: 1,500  
software engineers  
(working in consultation with pilots from thirty-seven  
airlines) had  
created a plane that could fly smoothly while carrying out  
tremendous  
feats of self-repair.

This contrasts the design of a submarine, where everything is  
exposed in an  
effort to show failure as soon as possible, with the design of a  
commercial  
airliner, where everything is hidden to always make the flight  
appear as  
smooth as possible to the passengers. I hadn't realized this  
smoothness may  
now extend to the airliner crew as well.

At any rate, it's a dramatic story that's worth reading.

Fred Ballard

## **⚡ D.01: Off by x100**

<George\_Robert\_Blakley\_III@tivoli.com>

*Mon, 28 Aug 2000 16:46:44 -0500*

I notice that both SmartMoney.com's "Map of the Market" and CNNfn's intraday chart have gotten confused by decimalization of stock prices. If you check out a decimalized stock (like Gateway (GTW), for example) at either of these sites:

<http://www.quicken.com/investments/charts/?symbol=GTW>

or

<http://www.smartmoney.com/marketmap/>

(and look at the largest block in the "Technology" sector)

you'll see that both sites think that Gateway's per-share valuation today (8/28) is \$6655.00, instead of \$66.55.

Bob Blakley, Chief Scientist, Tivoli SecureWay Business Unit

---

## **⚡ Western Union Web site hacked**

"Keith A Rhodes" <rhodesk.aimd@gao.gov>

*Mon, 11 Sep 2000 08:18:04 -0400*

Western Union warned thousands of online customers on 9 Sep 2000 that hackers had broken into the company's Web site. Although no fraudulent

transactions or breaches of personal information had been discovered, the penetration could have affected on-line users. More than 10,000 customers were being alerted, suggesting they cancel their credit and debit cards.

The Web site was out of service that evening, and was expected to remain that way for several days. [Source: AP item, 10 Sep 2000; PGN-ed]

---

## **✦ FBI arrests Emulex hoax suspect in Calif. (Re: Hoaxes, [RISKS-21.02](#))**

"NewsScan" <newsscan@newsscan.com>

*Fri, 01 Sep 2000 09:10:12 -0700*

A former employee of online press release distributor Internet Wire was arrested on 31 Aug 2000 and charged with securities and wire fraud in connection with the distribution of a phony press release that sent a tech company's stock price plummeting on 25 Aug. Shares of Emulex, a maker of fiber-optic equipment, lost up to 60% of their value, most of it during one 15-minute freefall, after some financial news services, including Dow Jones and Bloomberg, ran stories based on the release. The bogus release claimed the company had issued a profits warning, that it was being investigated by securities regulators, and that its CEO had stepped down. The stock eventually recovered most of its value after the company denied the reports. The suspect, 23-year-old Mark Jakob, allegedly used a

computer at  
El Camino Community College to construct and send the release,  
and then  
initiated a series of trades that netted him profits of \$240,000.  
(AP/\*Investors Business Daily\*, 1 Sep 2000; NewsScan Daily, 1  
September 2000  
<http://www.investors.com/editorial/tech05.asp>)

---

## **✶ Glitch at Amazon.com exposes e-mail addresses**

"Keith A Rhodes" <rhodesk.aimd@gao.gov>

*Mon, 11 Sep 2000 08:16:49 -0400*

Amazon.com apparently inadvertently released e-mail addresses of  
customers to  
Associates Program customers. It seems to be a Web script  
glitch.  
(Source: Item by Linda Rosencrance, 8 Sep 2000, Cable News  
Network, PGN-ed)  
[This followed shortly after Amazon announced a revision of its  
privacy  
policy that appears to have less protection for individual data.]

---

## **✶ Windows NT/2000 "Lock Computer" allows palm sync**

Avi Rubin <rubin@research.att.com>

*Fri, 8 Sep 2000 15:03:39 GMT*

In Windows NT and 2000, you can hit Alt-Ctr-Del, and one of the  
options is  
to lock the computer. Then, a password is required to unlock it.  
A reboot  
also requires a password to log in, so it would seem that this  
is a pretty

safe state to leave your computer in when stepping away from your desk.

The other day, I pushed the button to sync my palm pilot, and it worked.

Then I realized that I had locked my computer. I did some testing on Windows NT and 2000, and apparently, the Palm synchronization always works when the computer is locked.

There are several risks/attacks:

- I take a blank palm pilot to your computer, which is locked, and I sync with it and copy all of your palm pilot data. Many people keep a master list of accounts and passwords on their pilot, among other valuable/sensitive data.
- In a more malicious version of the previous attack, I sync all your palm data. Then, I zero out the contents of each record in every database. Then I sync again. The result is very likely that I will delete all of the data on the PC, and that the next time you sync, all of the data will be deleted on the palm. I know of a case where this "attack" worked in practice, by accident.
- I write a palm hack that does whatever I want it to do to your data. I then sync with your PC, and the hack gets copied to your pilot desktop. The next time you sync, the hack is installed on the palm.

I am sure there are other attacks that I haven't thought of. Anyway, I think that if Windows NT/2000 is going to have an option to lock the computer, it

must make access to something as important as all of the Palm Pilot databases inaccessible. Perhaps turn off access to the serial port, USB, port, etc, and not just the keyboard.

Avi <http://avirubin.com/>

---

## ✈ 1,000 system updates???

Scott Rainey <scottr@hevanet.com>  
*Mon, 28 Aug 2000 15:58:58 -0700*

This just in:

Microsoft Oregon Channel Update - September 2000  
Date: Mon, 28 Aug 2000 13:22:05 -0700  
From: Jennifer Kern <jennik@MICROSOFT.com>

<snip>

### IMPORTANT NEWS OF THE DAY

Microsoft Windows Update Corporate Website Launched Today!  
This site features more than 1,000 system updates and drivers for the Windows 2000 platform that can be distributed over a corporate network. It is a one-stop location for Windows Update content and Microsoft Windows Hardware Quality Lab logo device drivers. The site provides criteria-based searching based on vendor, operating system and device type.  
<http://corporate.windowsupdate.microsoft.com/en/default.asp>

## **✶ Risks of partially updated Web pages**

"Daniel P.B. Smith" <dpbsmith@bellatlantic.net>

*Sun, 27 Aug 2000 07:36:00 -0400*

eBay presents each auction on a bookmarkable Web page which shows the item description, the time remaining before the auction ends, the current high bid, and the eBay identity of the high bidder. On repeated access, the "time left" field decrements in near-real time, eventually changing to "Auction has ended."

The seller's guide notes that "Going, going, gone! When your auction ends, you and the high bidder will get e-mails." This breezy remark is the only thing the seller's guide says about these e-mails, and it is easy to assume that they are just reminders. In contrast, eBay is very emphatic about the importance of buyer and seller contacting each other "within 3 days" after the auction ends.

Formerly, confirmation e-mails were sent within a few hours of the close of the auction, but lately they have been very slow, taking, in some cases, several days to arrive.

I listed a cheap item on which I expected few bids and got single bid for my minimum price within a few hours after the auction started. Day by day the "time left" counted down, and eventually read "Auction has ended." The page still showed a single bid and the ID of the original bidder. Two days after close of auction I had not received any e-mail, so I contacted

the bidder  
shown on the Web page to initiate the transaction.

Needless to say, the next day a confirmation e-mail arrived showing that a second bidder with a higher bid had won the auction. The Web page for the auction, which formerly showed "Auction has ended, 1 bid, \$5.00" now showed "Auction has ended, 2 bids, \$12.50."

Obviously--in retrospect--the "time left" field is generated by some simple process that does not required database updating (since the end of the auction is constant). The rest of the page requires database access and is probably subject to the same delays as the process that sends the e-mail confirmations.

But it is natural to assume that if part of a dynamically generated Web page has been updated, the rest of it has, too. Stupid, to be sure--but natural.

---

## **✶ Re: Major security hole ... (van Keep, [RISKS-21.02](#))**

"Chris Adams" <chris@improbable.org>  
*Sun, 27 Aug 2000 12:14:16 -0700*

> If all of that is true, what value does the security audit  
that AA  
> performed have? [...]

If they're like the other big consulting firms, the security audits are designed solely to give upper management something to brag

about. We had a client site which got audited once by another big-name consulting firm. Since it was before the site launch, I was somewhat worried about this as the site was hosted on an NT box and I had yet to do my final security checks to verify that we'd closed all of the default wide-open security settings. After I had to explain some basic security concepts to the auditor when he didn't understand some of my questions about the sort of things they checked, I become rather less worried.

We passed with flying colors ("That's the most secure NT box we've ever seen - most of them are trivial to break into") and, having watched the server logs, all they looked for were some old security holes (e.g. :: \$DATA and a couple of microsoft sample security holes); their software engineering test appears to have been seeing whether your queries break when someone places a ' into a form. No attempts were made to do things like check for weak passwords or even test services other than WWW/FTP, much less anything resembling a serious attempt by a knowledgeable intruder.

Things like the URL editing attacks are something I use to show our greener new hires why they should always use a session libraries. The Annapa site appears to be using ASP and, while I have numerous complaints about ASP, a lack of built-in session support isn't one of them[1]. What this means is that whoever developed the site wasn't even at what I'd consider the "ASP for Dummies" level, which is deeply disturbing. The real irony, of course, is that it was more work for them to do things the way they did

than it  
would have been to do it the right way.

Chris Adams

[1] Of the platforms we deal with, ASP and ColdFusion have adequate session libraries and PHP has an excellent one (this relationship holds true for almost everything else). In all cases, sessions trivial to setup and use for basic tasks like the ones mentioned and even inexperienced developers will be up and running quickly.

---

## **✶ Re: Major security hole ... (van Keep, [RISKS-21.02](#))**

<zop12@mindless.com>

*Sun, 3 Sep 2000 18:30:05 -0700*

The reason why this happens so much is that programmers are coming from a centralised approach where the client side can be at least slightly trusted to an Internet based approach where everything is out in the open. I'll admit that I have to think really hard about how to perform my actions in such a way so as to keep everything in a session. Web programming is a different beast that many programmers are just not prepared to deal with.

They post information inside of hidden fields thinking it's safe. The only safe place is inside of a session object on your side, keyed by a random piece of garbage that you trail the client with (a session cookie) -- MD5

sums are great for this because they are a rather large  
keyspace, plus upon  
insert into the db you can check to make sure it's unique, and  
if not try to  
generate another session key.

The key itself cannot contain any data, but merely reference an  
internal  
data space, this is where many programmers go wrong. The key is  
made to be  
the data! This is utterly wrong and opens you to a host of  
problems. I  
even go so far as to drop into the local data what form entries  
\*should\* be  
if they are say modifying an existing record, I'll record little  
tuples of  
information that will allow me to later make sure that they  
aren't trying to  
sneak a change into another record ID. And yes this can be done  
in such a  
way so as to allow multiple browser windows. Yes it is  
complicated, but it  
must be done in order to maintain security.

Michael Loftis

---

## ⚡ **Re: Your TV is talking to your bracelet (NewsScan, [RISKS-21.02](#))**

George Weaver <weaver@gabriel.nso.psu.edu>

*Wed, 30 Aug 2000 18:13:13 -0400*

In [RISKS-21.02](#) we heard about Whispercode technology, which adds  
sub-audible  
coded signals to commercials that activate personal "hit"  
counters for  
measuring how many and perhaps which commercials a person has  
been exposed  
to. Hoping to increase the accuracy of measuring the

effectiveness of TV advertising, Whispercode's CEO is quoted as saying "With Whispercode, we will finally be providing our clients with a true accounting of where their advertising money is going."

By "tagging" commercials like this, Whispercode may have inadvertently provided what has historically been carefully avoided by the television industry - a signal that distinguishes commercials from "content". The availability of this information will make it trivial to develop the much sought "commercial killer" box. This may produce the further unintended effect of proving beyond a doubt where advertisers' money is going - straight down the drain.

---

## **✶ PFIR statement on government interception of Internet data**

Lauren Weinstein <lauren@vortex.com>  
*Thu, 7 Sep 2000 17:49:37 -0700 (PDT)*

The PFIR (People For Internet Responsibility) statement dated September 7, 2000, entitled:

"PFIR Statement on Government Interception of Internet Data"

is available at:

<http://www.pfir.org/statements/interception>

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

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

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

---

## ⚡ **REVIEW: "Big Book of IPsec RFCs", Pete Loshin**

Rob Slade <rslade@sprint.ca>

*Mon, 11 Sep 2000 11:23:13 -0800*

BKBBIPSR.RVW 20000614

"Big Book of IPsec RFCs", Pete Loshin, 2000, 0-12-455839-9,  
U\$34.95/C\$48.95

%E Pete Loshin pete@loshin.com

%C 340 Pine Street, 6th Floor, San Francisco, CA 94104-3205

%D 2000

%G 0-12-455839-9

%I Morgan Kaufmann Publishers

%O U\$34.95/C\$48.95 415-392-2665 fax: 415-982-2665 mkp@mkp.com

%T "Big Book of IPsec RFCs: Internet Security Architecture"

RFC (Request For Comments) documents are the standard references of the

Internet. (Not that all of them are standards as such: some are discussion

papers or even opinion pieces. RFC 1796 has an interesting take on this

fact.) IPsec is that group of articles dealing with security.

The RFCs are

important materials. They are also available online, for free.

Why, then,

would you pay for a collection of them?

Fortunately for the ease of my review, Loshin asks this question, and gives

a detailed answer, in the introduction. In the first place, you'll probably

want to print out the documents at some time, and this is

probably one of the cheapest ways to do it. (Certainly one of the most convenient.) Also, this is a collection of the IPsec standards, and therefore the compilation work has been done for you. Finally, Loshin has provided an extensive index, which greatly increases the value of the text. (Original formatting has been retained, and the individual manuscripts preserve their page numbering: the index can be used to point to items in the RFCs even for those referring to the online forms.)

Twenty three RFCs are included in the book. Fortunately for Loshin's effort, one of the documents provides an overview of net security and another presents a structure for the RFCs themselves. Each contains its own definitions of terminology, although an aggregated glossary would have been helpful. The items are listed in numerical order, as is suitable for a reference work: RFC 2401, on security architecture, is possibly the best starting point for newcomers, but is roughly in the middle of the book, and RFC 2411, describing the relationships among the RFCs, comes near the end.

Topics include the MD4 and MD5 digest algorithms, using MD5 for IP authentication, ESP (Encapsulating Security Payload) encryption, RC5 encryption, hashed message authentication code (HMAC), the CAST-128 algorithm, test cases for message digests, RC2 encryption, security architecture, the authentication header, Internet Security Association and Key Management Protocol (ISAKMP), security associations,

## Internet Key

Exchange (IKE), NULL encryption, a document roadmap, OAKLEY key determination, and the Diffie-Hellman key agreement method.

For those needing, or even wanting, to know about IPsec, this is the reference.

copyright Robert M. Slade, 2000    BKBBIPSR.RVW    20000614  
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>

---

## 2001 IEEE Security and Privacy Symposium

Jon Millen <millen@csl.sri.com>

*Mon, 28 Aug 2000 13:52:35 -0700*

The announcement and call for papers are at:

<http://www.ieee-security.org/TC/sp2001.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 21: Issue 5**

**Weds 20 September 2000**

## Contents

- [Qualcomm CEO's laptop vanishes, containing corporate secrets](#)  
[NewsScan](#)  
[David Lesher](#)
- [Computers shut down aircraft engines in flight](#)  
[Mike Beims](#)
- [Russian troops block power shutoff](#)  
[Doneel Edelson](#)
- [OPEC site hacked](#)  
[Mike Hogsett](#)
- [Navy carrier to run Win 2000](#)  
[Mike Ellims](#)
- [Re: Windows NT/2000 palm sync](#)  
[Avi Rubin](#)
- [Re: Identity theft](#)  
[Carl Ellison](#)
- [Re: D.01: Off by x100](#)  
[Terry Carroll](#)
- [Re: New Pentium III chip recalled: typo](#)  
[Gideon Yuval](#)
- [Risks of using HTML Mail and HTTP proxy "censorware" together](#)

[Dan Birchall](#)

- [Concorde crash report](#)  
[Peter Kaiser](#)
  - [Computerized air-conditioning risks](#)  
[Pere Camps](#)
  - [``Netspionage" is the real security threat on the Net](#)  
[NewsScan](#)
  - [Hackers offered \\$10,000 bait](#)  
[NewsScan](#)
  - [A subtle fencepost error in real life](#)  
[Andrew Koenig](#)
  - [New credit-card solution?](#)  
[Joshua M Bieber](#)
  - [Reconstructing Privacy - Conference Announcement](#)  
[Gene N Haldeman](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

## ✶ **Qualcomm CEO's laptop vanishes, containing corporate secrets**

"NewsScan" <newsscan@newsscan.com>

*Mon, 18 Sep 2000 06:55:57 -0700*

After addressing a national business journalists' meeting in Irvine, California, Qualcomm chief executive Irvin Jacobs found that someone had stolen his laptop computer, which he left on the floor of a hotel conference room. The thief acquired not only an IBM Thinkpad but also the Qualcomm secrets it contains, because Jacobs had just finished telling the audience that the slide-show presentation he was giving with his laptop contained proprietary information that could be valuable to foreign governments. People in the area "included registrants, exhibitors and guests

at our conference, hotel staff and perhaps others.' Qualcomm, a leader in the wireless industry, and is the world's leading developer of a technology known as CDMA, which makes high-speed Internet access available on wireless devices. (Reuters/\*San Jose Mercury News\*, 18 Sep 2000 <http://www.sjmercury.com/svtech/news/breaking/ap/docs/4122581.htm>; NewsScan Daily, 18 September 2000)

NewsScan Daily is underwritten by Arthur Andersen and IEEE Computer Society, world-class organizations making significant and sustained contributions to the effective management and appropriate use of information technology. NSD is written by John Gehl and Suzanne Douglas, editors@NewsScan.com. [NewsScan items are reproduced here with the very gracious permission of Gehl and Douglas. Further reuse should respect their copyrights. PGN]

---

## **Qualcomm CEO's laptop vanishes, containing corporate secrets**

David Lesher <wb8foz@nrk.com>  
*Mon, 18 Sep 2000 22:36:02 -0400 (EDT)*

This was bound to happen, if not then & there and to him, then to another CEO-type. It will again. It's a clear message that folks of all levels need to practice safe-computing by using real encryption on all data files.

It's also a message to crypto companies. Create real tools for

this task,  
ones that even C[E,F,T]O's can grok how to use {1}. A recent USENIX study reported that a large percentage of users failed to use PGP correctly.

{1: Getting them to follow practices is the 2nd half of the problem; as the Deutch case demonstrates....}

wb8foz@nrk.com [v].(301) 56-LINUX

---

## ✶ Computers shut down aircraft engines in flight

Mike Beims <mbeims@mail-fair.ivv.nasa.gov>

*Mon, 18 Sep 2000 15:57:01 -0400*

The Aerospace Online newsletter reports that some Full Authority Digital Engine Control (FADEC) units have performed uncommanded shut downs of an aircraft's engine in flight. This led to the United State's Federal Aviation Administration issuing an Airworthiness Directive (AD) requiring that no more than one engine per airplane may use the suspect FADEC's.

The root cause of the FADEC computer malfunction is a power transistor, and the AD lists the FADEC units affected by their serial numbers.

From <http://www.aerospaceonline.com>:

2) AD released on Allison AE 3007A/C series turbofan engines FAA adopted a final rule applicable to Allison Engine Company AE 3007A and AE 3007C series

turbofan engines that requires inspection before further flight to determine that no more than one engine with a suspect FADEC is installed on the same airplane. The rule was prompted by reports of uncommanded in-flight shutdowns of engines caused by a potential hardware failure mode in some AE 3007 series FADECs. The rule is effective 22 Sep 2000.

The AD text (.pdf) is available from Aerospace Online's Download Library:

<http://www.aerospaceonline.com/read/nl20000912/213768>

Mike Beims <Mike.A.Beims@ivv.nasa.gov>

---

## **✶ Russian troops block power shutoff**

Doneel Edelson <doneel.edelson@eulergroup.com>

*Tue, 12 Sep 2000 15:53:29 -0400*

A Russian strategic missile base had its power shut off as a result of a year-long accumulated nonpayment of bills totalling about \$683,000. As a result, troops took over the utility's switching station and restored power. Earlier shutdowns affected hospitals, an air-traffic control center, coal mines, a city sewage plant, and in 1995 a nuclear submarine at an Arctic sub base. [Source: Associated Press article by Vladimir Isachenkov, 12 Sep 2000, PGN-ed]

---

## **⚡ OPEC site hacked**

Mike Hogsett <hogsett@blob.csl.sri.com>

*Wed, 13 Sep 2000 11:08:41 -0700*

Someone identified as "fluxnyne" cracked into the OPEC Web site, posting

this message: "I think I speak for everyone out there (the entire planet)

when I say to you guys to get your collective a\*\*es in gear with the crude

price. We really need to focus on the poverty-stricken countries, who don't

even have enough money for aspirin, let alone exorbi[t]ant prices for

heating oil. I think the lives of children are paramount to your profits."

[[http://dailynews.yahoo.com/h/nm/20000913/od/website\\_dc\\_1.html](http://dailynews.yahoo.com/h/nm/20000913/od/website_dc_1.html),

PGN-ed

with \*\* filtering]

---

## **⚡ Navy carrier to run Win 2000**

Mike Ellims <mike.ellims@potechnology.com>

*Wed, 20 Sep 2000 09:27:47 +0100*

Apparently the new Navy aircraft carrier is to use windows or some

derivative for at least some of it's mission critical applications.

"This is a new area for us," said Keith Hodson, a Microsoft Government

spokesman. "Windows-based products have not traditionally been associated

with Defense Department-specific mission-critical applications."

The Web site with the press release:

[http://www.gcn.com/vol19\\_no27/dod/2868-1.html](http://www.gcn.com/vol19_no27/dod/2868-1.html)

As they say, who do you want to shoot today?

Mike Ellims, Pi Technology mike.ellims@pitechnology.com  
www.pitechnology.com +44 (0)1223 441 434

---

## ✦ **Re: Windows NT/2000 palm sync (Rubin, [RISKS-21.04](#))**

Avi Rubin <rubin@research.att.com>

*Mon, 18 Sep 2000 19:59:26 -0400*

Some people have pointed out that a virgin palm pilot would cause a pop-up window asking for the user name, so for the attack that I mentioned to work, you would have to know the username on the pilot of the person you were attacking, and set that name in the new palm. It was also pointed out that the palm databases can be backed up, in which case obviously data wouldn't be lost. There may have been a few other problems with the hypothetical attacks I mentioned. However, the main risk remains - that locking a windows machine with the alt-ctrl-del option does not prevent the palm from syncing, and you can imagine ways in which this can be abused in additions to the ones I mentioned in the original post.

Perhaps disabling the serial port would be a bit draconian. Then what about the Ethernet port? What if someone wants to receive a fax while they are away, but lock the computer? Where do you draw the line between

locking the computer and turning it off? These are difficult questions. I believe the sync issue when the computer is locked is a user interface problem, and yet, everyone that I tell about being able to sync the pilot after locking windows 2000 is surprised. Locking the computer is a useful feature, but it needs to be done in such a way that the user has an intuitive sense of what is locked and what isn't. I don't have the solution.

Avi Rubin <http://avirubin.com/>

---

## ✶ Re: Identity theft (PGN, [RISKS-21.04](#))

"Carl Ellison" <cme@acm.org>  
*17 Sep 2000 19:16:23 -0700*

I used to try to keep my SSN private -- then I realized that that's blaming the victim (me). It's not the SSN holder's fault that stores and other institutions use improper means for authenticating people. It's the store's fault.

Any information held by a credit bureau is public. So is any information held by any government agency, if I'm to believe the spam I get occasionally.

So, that information is not acceptable for authentication -- even in person, but especially online. It's not merely unacceptable when dealing with the credit bureau. The credit bureau poisons the information for

everyone.

Now -- how do we get consumer protection laws that make it clear that a consumer is not liable for any debts incurred by someone claiming to be him/her unless there is irrefutable authentication during registration (e.g., videotape of the consumer signing up for the service). This means killing all issuing of credit online, by mail, by phone, etc.

Maybe I'd stop getting all those credit-card applications in the mail....

[This opens a technical challenge: how can we authenticate anyone, if we rule out information that an attacker can get?]

- Carl

[This topic has recurred in RISKS for many years, but the people who should be learning this lesson are not listening (or lessening -- although they may be lessening). Thus, your moderator not at all immoderately includes Carl's contribution. PGN]

---

## **⚡ Re: D.01: Off by x100 (Blakley, [RISKS-21.04](#))**

Terry Carroll <carroll@tjc.com>  
*Mon, 11 Sep 2000 15:41:20 -0700 (PDT)*

> I notice that both SmartMoney.com's "Map of the Market" and CNNfn's  
> intraday chart have gotten confused by decimalization of stock prices.

> If you check out a decimalized stock (like Gateway (GTW), for example)  
> at either of these sites ... you'll see that both sites think that  
> Gateway's per-share valuation today (8/28) is \$6655.00, instead of  
> \$66.55.

This is not (to the best of my knowledge) a decimalization issue, but for an interesting computer error related to stock price, check out the quote for Ford Motor Company (ticker symbol F) on Yahoo.

The data includes a spurious split of Ford stock on August 3, 2000: a "-44:-24" split (or, on some screens, such as the historical data referred to below, a "1748:1000" split). However, there was no split on that date: instead, there was a stock drop due to the Firestone tire problems.

You can see this most clearly by viewing a stock chart at <http://finance.yahoo.com/q?s=F&d=3mm>. Yahoo shows Ford as jumping from around \$26.50 (pseudo-split-adjusted) to around \$29 (a 9% increase) on August 3. In reality, it dropped like a stone, from around \$47 \*down\* to around \$29 (a 45% DECREASE). Yahoo is split-adjusting for this non-existent split.

The problem is also visible in the historical charts page, e.g., on <http://chart.yahoo.com/d?s=f>.

I suspect that there's some program somewhere that treats such a precipitous overnight stock price drop as a potential split, although why it's not referred to a human for verification, and why it settles on such odd ratios eludes me.

I reported the error to Yahoo a couple weeks ago. They said that they'd notify their data provider (CSI Data), who would verify and correct, and that sometime in the future, the displays at Yahoo would again be correct. It's still not correct.

In the meantime, I hope that no Yahoo users are trying to rely on moving averages or other historical bases to try to figure out a good time to trade in Ford.

Terry Carroll, Santa Clara, CA [carroll@tjc.com](mailto:carroll@tjc.com)

---

## ⚡ **Re: New Pentium III chip recalled: typo ([RISKS-21.04](#))**

Gideon Yuval <[gideony@microsoft.com](mailto:gideony@microsoft.com)>

*Tue, 12 Sep 2000 15:02:15 -0700*

> Intel is recalling its 1.3 gigahertz Pentium III chip

I think it was 1.13GHz, not 1.3

---

## ⚡ **Risks of using HTML Mail and HTTP proxy "censorware" together**

Dan Birchall <[djb0x7736fb0b@scream.org](mailto:djb0x7736fb0b@scream.org)>

*20 Sep 2000 01:56:30 GMT*

Summary: Unseen things in HTML mail may trigger HTTP censorware.

First, the data points:

1. Many workplaces, including mine, have HTML-"enabled" mail software on the desktop.
2. Many workplaces (though not as many), including mine, make use of HTTP proxy "censorware" to catch employees trying to access "bad" sites (porn, hate sites, hacking sites, etc).
3. Those sites, like many others, tend to use 1x1 GIFs for spacing and the like.
4. Users who read HTML mail rarely view the source.

Now, the risk:

It is extremely trivial to concoct an HTML mail message containing IMG SRC calls to (near-)invisible 1x1 images, or other more damning images scaled to 1x1, from any number of "banned" sites.

If such a message is received and opened by someone with an HTML mail reader, they will probably generate HTTP requests to those sites, which would be blocked/logged by proxy censorware.

Thus, a prankster, BOFH, or anyone bent on malice can pull off a "joe job" by sending e-mail to such a recipient. The e-mail might appear to be totally innocent based on its content, or might even be disguised as spam, with forged headers and other junk.

It doesn't matter, really, as long as the recipient's mailreader generates the HTTP requests for those files. Enough entries in the censorware log

over a period of time, and someone's bound to start asking questions.

Of course, the HTTP requests are for individual files, not pages. But if the proxy is blocking requests to "banned" sites (ours is), no pages could be accessed anyway, so all log entries would be of an individual-file nature. These are just blocked requests for images, rather than blocked requests for HTML files.

(As a side note, if someone were ideologically opposed to the use of censorware, sending this sort of message to a large number of users behind such a proxy, including those parties charged with administering the proxy, would seem to be a fitting form of protest.)

Dan Birchall - Palolo Valley, Honolulu HI - <http://dan.scream.org>  
Post your reviews; get paid: <http://epinions.scream.org/join.html>

---

## **✈ Concorde crash report**

Peter Kaiser <kaiser@acm.org>  
*Tue, 12 Sep 2000 21:52:01 +0200*

The Bureau Enquêtes-Accidents (BEA; Office of Accident Investigation) has issued a preliminary report on the Concorde crash of 25 Jul 2000. It may be worth mentioning a couple of things here.

One is that the crew apparently never knew what was wrong, because there was no means of sensing the actual problem: the catastrophic rupture

of a fuel tank caused by the explosion of a tire, with massive ignition of the leaking fuel. The Concorde's engines are instrumented to detect fire, but the tanks are not; nor is there any means of detecting the rupture of a tank nor of extinguishing a tank fire. And the pilots couldn't see to the rear. So all the sensors were no use at all, and the flight was doomed before it left the ground. Undoubtedly the passengers on the left side of the plane could see the flames and the disintegration of the left wing.

There's a parallel here to the instrumentation of computer systems in places, and at levels, that make it possible to diagnose problems before they result in catastrophe.

The aircraft carried three types of recorders. The cockpit voice recorder had external damage, but its thermal protection worked and its tape was recovered intact. The flight data recorder (FDR) didn't entirely protect its tape from fire, and the report states that its

... recording was of moderate quality, which led to a certain number of losses of synchronization of the signal.... It was decided to search in parallel for better-quality information.

They turned to the quick-access recorder (QAR, in French literally "maintenance recorder"), which is not required equipment:

The QAR is an unprotected recorder. It contains a copy of the FDR's data on magneto-optical disk, and is used by Air France to analyze flights.

The method of writing on this disk uses three buffer memories whose role is to store data sent by the Flight Data Acquisition Unit (FDAU) until the conditions of vibration detected by an accelerometer within the QAR are favorable to write on the disk. These are volatile memories which must be supplied with current to preserve the information they contain....

The QAR's box was crushed and the magneto-optical disk deformed. The card holding the memories, visible through the half-torn-off cover, seemed to be in good condition. Thus it was decided to concentrate work on this card. Two of the three memories had been torn off at the impact. The third was still in place and powered.

No one had ever before tried to recover one of these memory units live from a damaged recorder, but after some experimentation on other units, by attaching the third memory to a parallel power supply they managed to move it intact and operational to a working card.

The contents of the third memory ... could be read and a copy of the disk was sent to the BEA [where] it became clear that the data from this flight were to be found on the only one of the three memories that had remained powered. Because of the technology used, the quality of the recording was excellent and displayed no desynchronization. Thus it was unnecessary to try to read the magneto-optical disk, nor to proceed with new work to acquire a [usable] signal from the FDR's tape.

So the flight data recorder didn't survive the crash unharmed, but a perfect recording was recovered from the volatile digital medium within an unprotected, vibration-sensitive, optional recorder.

The preliminary report, "Accident survenu le 25 juillet 2000 au lieu-dit La Patte d'Oie de Gonesse (95) au Concorde immatriculé F-BTSC exploité par Air France", is BEA document f-sc000725p, available from BEA's Web Site (only in French). All quotations above are my translations, for whose quality I beg your forbearance.

---

## ✈ Computerized air-conditioning risks

Pere Camps <pere@pere.net>  
*Tue, 19 Sep 2000 19:45:05 +0100 (BST)*

We just moved offices this monday to a brand new building and we found out, the hard way, that the air-conditioning machines were working much too well: we were freezing.

This surprised most of us, as the new AC system was ran by a PC and it had a very user-friendly interface. It looked very robust.

However me, being a long time RISKS follower, knew that having a PC for controlling your AC wasn't necessarily A Good Thing (TM).

After some "debugging", we found out that the control software was buggy. We notified this to the appropriate vendor which confirmed the bug with us and

told us that it would be soon be fixed.

In the meantime, we have to work with gloves and the coat on...

[Added note: The bug with the PC software was so huge (it looks like it

only happens with our setup - the vendor claims is the first time it

happens), that what we have is the AC units running continuously, no

matter what the thermostat tells the control unit.

Good thinking that our department (MIS Support & Internet) was the only

one that stayed behind and will move in three weeks time. We know that is

not good to be beta testers of v1.0 "hardware and software" (ie, building).]

---

## **⚡ "Netspionage" is the real security threat on the Net**

"NewsScan" <newsscan@newsscan.com>

*Tue, 12 Sep 2000 10:58:35 -0700*

Teenage hackers who deface government sites or steal credit-card numbers

attract a lot of attention, but experts say the real problem of cybercrime

is corporate-sponsored proprietary information theft committed by professionals who rarely get caught. According to the American Society for

Industrial Security, Fortune 1000 companies sustained losses of more than

\$45 billion last year from thefts of proprietary information, and a survey

by the Computer Security Institute indicates over half of 600 companies

polled said they suspected their competitors were a likely source of cyberattack. "Your competitors no longer have to be across town, or even across the country; they're in other countries that have different laws and business ethics," says Richard Power, who conducts the annual CSI survey. "Culpability is much less. There is a lawless frontier in terms of theft of trade secrets." Experts agree that while juvenile hackers often leave calling cards enabling them to be traced, professional information thieves are almost impossible to catch. What's even more frustrating is that many firms never know their systems have been breached. "It's difficult for people to see the theft of information," says the owner of a security firm. "Information is the only asset that can be copied or stolen but nothing can appear to be missing. You can still have the information... but have lost the value of that information." (MSNBC, 11 Sep 2000 <http://www.msnbc.com/news/457161.asp>; NewsScan Daily, 12 September 2000)

---

## **🔥 Hackers offered \$10,000 bait**

"NewsScan" <newsscan@newsscan.com>  
*Wed, 13 Sep 2000 08:18:25 -0700*

The Secure Digital Music Initiative, a forum of 175 companies in the music, electronics, information technology and telecommunications industries dedicated to developing a secure framework for the digital

distribution of music, is offering a reward of up to \$10,000 to the first person to crack its codes. In an open letter to the "alternative" press, SDMI executive director Leonardo Chiariglione challenged hackers to "show off your skills, make some money, and help shape the future of the online digital music economy." SDMI has about 10 different proposals for "watermarking" technology that could be embedded in a digital music file. Portable music players complying with the SDMI standard would only work if the watermark -- an inaudible signal -- is present. SDMI has also issued the challenge to the technology departments at the University of California at San Diego, MIT, Virginia Tech and Stanford University. "The proposed technologies must pass several stringent tests: they must be inaudible, robust and run efficiently on various platforms, including PCs... So here's the invitation: Attack the proposed technologies. Crack them. By successfully breaking the SDMI protected content, you will play a role in determining what technology SDMI will adopt," said Chiariglione. (\*Financial Times\*, 13 Sep 2000 <http://news.ft.com/news/industries/media>; NewsScan Daily, 13 September 2000)

---

## **✶ A subtle fencepost error in real life**

Andrew Koenig <[ark@research.att.com](mailto:ark@research.att.com)>  
*Wed, 20 Sep 2000 15:15:49 -0400 (EDT)*

I recently got email from amazon.com offering me a \$50 discount on any order of \$100 or more from ashford.com. As it happens, my wife's wristwatch needed repair, and I decided that for \$50 I wouldn't mind buying her another watch if I could find one I thought she would like.

I found such a watch, for exactly \$100. When I tried to order it, the ashford.com website wouldn't accept my promotional-offer code. More precisely, it accepted it but didn't indicate any discount.

So I called them on the phone. The (very pleasant) sales rep said that he could place the order for me. When he tried, though, he also found that their system wouldn't accept the promotional code.

He then told me that he would go ahead and place the order anyway, and once it was in their system, he would make sure that I was charged the right price. It might take a day or two, but he would make it right. I told him to go ahead.

They let you track existing orders on their website. Later that day, the order was there, showing a price of \$100.00. The next day, it still showed \$100.00. The following day, it showed \$50.01.

If you've read this far, I trust that you can figure out what must have happened.

Andrew Koenig, ark@research.att.com, <http://www.research.att.com/info/ark>

[I can only assume that the resourceful sales rep added \$0.01 to

the price, in order to cater to a system that was implemented to offer the discount only for orders strictly greater than \$100, rather than the \$100 or more promised in the promotional email. ARK]

---

## ✶ New credit-card solution?

"Joshua M Bieber (852-5436)" <jbieber@vnet.ibm.com>  
*Tue, 12 Sep 00 09:47:43 EDT*

Safer online shopping with disposable credit cards

American Express will launch a disposable credit-card service in the US next month, designed to answer the worldwide worry of online shopping. The system, Private Payments, enables cardholders to access a random one-use only credit-card number with an expiry date on the AmEx website, to be used in making one online purchase. In the event that the number is illegally accessed during a transaction, it cannot be re-used by a hacker. Visa and Mastercard are also looking at similar ideas.

\*The Independent Monday Review\*, P9, \*The Mirror\*, P18

[Not comforting! JMB]

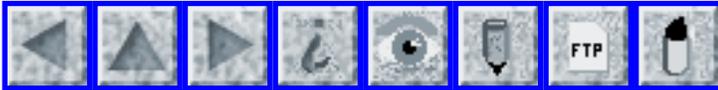
---

## ✶ Reconstructing Privacy - Conference Announcement

Gene N Haldeman <geneh@cpsr.org>  
*Sat, 16 Sep 2000 19:08:48 -0400*

CPSR will hold it's Annual Meeting for 2000, "Drawing the Blinds: Reconstructing Privacy in the Information Age", October 14 & 15 on the campus of the University of Pennsylvania in Philadelphia. Marc Rotenberg of EPIC will be receiving our Norbert Wiener award, and Dave Farber will be keynoting. More info and registration is at <http://www.cpsr.org/conferences/annmtg00/>.

Gene N Haldeman <cpsr@gene-haldeman.com> Mid-Atlantic Regional Director,  
Computer Professionals for Social Responsibility



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 21: Issue 6**

**Monday 25 September 2000**

## Contents

- [Australian online voting scores: no oohs 'n Oz?](#)  
[Garry Allen](#)
- [Youthful toothful](#)  
[PGN](#)
- [Concorde Problem Visibility](#)  
[Peter B. Ladkin](#)
- [Re: Concorde crash report](#)  
[Zygo Blaxell](#)
- [Ostrich Farming?](#)  
[Pat St-Arnaud](#)
- [Pentagon security gate goof, again](#)  
[PGN](#)
- [U.Wisconsin alters photo to add "diversity" to student body](#)  
[PGN](#)
- [Why software fails](#)  
[Mike Lewis](#)
- [Filtering, censorship, silence: Who owns the language?](#)  
[Richard Schroepel](#)
- [Re: Decimalization and Ford Stock Splits](#)  
[Timothy Prodin](#)

- [Re: Identity theft](#)  
[Martin Minow](#)
  - [Re: Qualcomm CEO's laptop vanishes](#)  
[Camillo Sars](#)
  - [Re: Risks of using HTML Mail and HTTP proxy "censorware" together](#)  
[J.D. Abolins](#)
  - [Artificial Intelligence strikes again](#)  
[Rodger Whitlock](#)
  - [SBC Calling Card PIN](#)  
[Conrad Heiney](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

## ✶ Australian online voting scores: no oohs 'n Oz?

Garry Allen <GAllen@dspmedia.com.au>

*Thu, 21 Sep 2000 14:49:59 +1000*

The Australian Broadcasting Corporation ran a television show recently called Race Around Oz. It was a competitive documentary series where 6 competitors had to present a five minute documentary every two weeks. These were then judged by industry representatives as a story with the overall winner receiving a digital video camera and a two week stint as a producer on one of the ABC documentary shows.

There was also an audience winner. Viewers were invited to vote either by toll number or by an online voting form. The audience winner also received a video camera and a two week stint. Apparently there was nothing to stop someone voting early and voting often. The ABC also has a show looking at the media, Mediawatch. For some reason, the audience voting

patterns were brought to the show's attention. The winner of the audience vote was 5 times as popular as any of the other contestants in the online votes despite her documentaries being hated by the judges. In fact, according to the program transcript, they asked the School of mathematics at the Swinburne University of technology to investigate. they found that the difference in online voting patterns being solely due to chance to be statistically significant at the 1% level, ie highly unlikely. Mediawatch did some research and has raised some questions about the results.

<http://www.abc.net.au/mediawatch/transcripts/s175489.htm>

<http://www.abc.net.au/mediawatch/transcripts/s181183.htm>

The comments quoted below are pertinent.

From the first show:

- > ABC Online say they're working on the problem but warn: The ABC is aware
- > that online voting does have limitations ... such voting should never be
- > construed as an accurate representation of an entire audience or
- > population's views. (ABC Online e-mail to Media Watch 8/9/00)
  
- > Paul Barry: And that's a warning that Race Around Oz might take on board
- > before they rely on their online votes again.
  
- > As Jane put it: Thanks for coming with us for what has been the ride of a
- > lifetime for everyone involved with the program ... (ABCTV Race Around Oz
- > final episode)
  
- > Paul Barry: Or maybe - thanks for letting us take you all for

the ride of  
> a lifetime.

And from the second show:

> So what will the ABC be doing about this? The ABC will, of course, look  
> closely at the allegations and at all documentation before deciding on a  
> course of action. (Race Around Oz fax to Media Watch 18 Sep 2000)

> Paul Barry: Yes. And when they've worked out what to do about Stacey,  
> they'd better take a closer look at what to do about their own reliance on  
> a voting system that is so easily abused.

It is hard to believe that an online voting system could ever be manipulated like this, particularly not one associated with a reputable media organisation such as the ABC. (:--)) And no doubt the e-mails purporting to be from Stacey could have been forged. But somehow I doubt that the organisers of Race Around Oz will use a voting system like this again.

Garry Allen

---

## Youthful toothful

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

*Wed, 20 Sep 2000 19:52:21 PDT*

On 20 Sep 2000, Jonathan Lebed, 15, settled a federal civil-fraud process, agreeing to pay \$272,826 for perpetuating bogus information on the Internet that led to the stock fluctuations in Just Toys Inc. and The

Havana Republic  
and profiting therefrom.

On 21 Sep 2000, Jonathan James (cOmrade), 16, pleaded guilty to two counts of juvenile delinquency and was sentenced to six months detention for having penetrated DoD and NASA computer systems, intercepting 3,300 e-mail messages and stealing passwords. (He was 15 at the time. If he had been an adult, he reportedly would have received a sentence of at least 10 years.)

On 21 Sep 2000, Jason Diekman, 20, was charged with cracking into university (including Harvard, Stanford, and Cornell) and NASA computer systems, and stealing hundreds of credit-card numbers to buy thousands of dollars of clothing, stereo equipment, and computer hardware.

(Also, the Emulex stock manipulation case was noted in [RISKS-21.02.](#))

[Sources include an article by David Stout, \*The New York Times\*, 23 Sep 2000, National Edition A9, plus AP item 22 Sep 2000.]

---

## ✶ Concorde Problem Visibility (Kaiser, [RISKS-21.05](#))

"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>  
*Thu, 21 Sep 2000 11:14:39 +0200*

> Undoubtedly the passengers on the left side of the plane could see  
> the flames and the disintegration of the left wing.

Let me doubt it. The fuel leak came from under the wing approximately adjacent to the main gear and streamed backwards, burning in the process. The Concorde wing is a delta (unique among in-service passenger transports) and extends some meters rear of the last passenger cabin window. Airflow under the wing is rearward during takeoff, flight and landing; in particular it may be seen on the still pictures and video how the burning fuel streamed.

As far as I know, the left wing did not "disintegrate" until impact (but that depends on what "disintegrate" means).

These observations, however, go to substantiate Kaiser's point that the evidence of the problem was sparse to those on board.

Kaiser recounts the retrieval of evidence from various recorders. The issues concerning installation and use of recorders are broadly thus. Recorders are fallible devices, depending on what happens in the accident. More recorders mean more complex devices to go wrong, potentially hindering normal operations (fully working recorders are required for any normal operations); and more complex devices to attempt to analyse in a partly-destroyed state; finally, more discrepancies to resolve if their readings don't all cohere. External video recorders have been proposed, mainly to help resolve gear problems and other problems the pilots can't see (1979 DC-10 in Chicago; Concorde). Cockpit video recorders (which I call CVidR) have been proposed, and recommended by certain safety watchdog authorities. While they may have some benefits in identifying

what was actually on frangible CRT displays at the time of an incident (2000 Crossair crash in Zuerich), pilots are concerned that the presence of CVidR may hinder their competent conduct of the flight in normal operations as well as in emergency situations; not only that, but that CVidR evidence could broaden the possibilities for civil litigation in directions detrimental to air travel as a whole.

Peter Ladkin

---

## ✈ Re: Concorde crash report (Kaiser, [RISKS-21.05](#))

Zygo Blaxell <uryse0d5@umail.furryterror.org>

*21 Sep 2000 19:50:53 -0400*

> No one had ever before tried to recover one of these memory units live  
> from a damaged recorder ... they managed to move it intact and operational  
> to a working card.

I hope that "no one had ever before" refers to retrieving data from that specific type of memory unit or from that specific type of recorder, because anything less specific is inaccurate. ;-) I know of at least two previous incidents of flight data extracted from memory devices on crashed aircraft.

One company was able to extract engine data from a memory device on the same aircraft, but unfortunately the only press copy available

to the  
public I can find for that device isn't very specific:

<http://www.airdisaster.com/news/0500/25/news3.html>

In the other case the circuitry around the memory was damaged,  
and it  
was necessary to repair this damage (microsurgery with an FIB)  
without  
disturbing the contents of the memory:

<http://www.chipworks.com/News/11Swissair.htm>

> So the flight data recorder didn't survive the crash unharmed,  
but a  
> perfect recording was recovered from the volatile digital  
medium within an  
> unprotected, vibration-sensitive, optional recorder.

It just goes to show that more is usually better when it comes to  
redundant storage devices on mission-critical systems. ;-)

---

## ✶ Ostrich Farming?

Pat <pat@machome.com>

*Thu, 21 Sep 2000 14:20:42 -0400*

I would find it funny if it was not so scary: I thought I was  
doing the  
responsible thing when I sent a special notification to our  
subscribers, an  
article and link to a recent CERT advisory bulletin regarding a  
potential  
upcoming DDoS, and what to look for in a server audit. Albeit I  
knew there  
was many readers to whom this would not be of any use, we also  
have a lot of  
system managers on board. I felt ready and able to answer a

predicted flood  
of questions this would generate. I was actually glad of the  
opportunity to  
sensitize some people to the issue of network security.

What I DIDN'T EXPECT were the numerous flames that would follow!

I was called by all possible names, accused of sending SPAM or  
disseminating  
rumors.

Six months have elapsed since last February's massive distributed  
denial-of-service attacks, yet the following article reports  
that there are  
still over 100,000 vulnerable computers all around. With  
billions of dollars  
of lost business, one would think people would take the issue  
more  
seriously!

See <[http://www.internetnews.com/bus-news/  
article/0,2171,3\\_436031,00.html](http://www.internetnews.com/bus-news/article/0,2171,3_436031,00.html)>

Pat St-Arnaud, Editor, MacHome Journal's Hot Tips Weekly  
pat@machome.com  
www.machome.com

---

## **⚡ Pentagon security gate goof, again**

"Peter G. Neumann" <neumann@csl.sri.com>  
*Sun, 24 Sep 2000 11:46:52 PDT*

In [RISKS-19.97](#), we reported on a Pentagon security system that  
injured the  
visiting Japanese Defense Minister and five others when a  
barricade was  
raised at the wrong time, in September 1998. That accident was  
attributed

to a faulty sensor, and resulted in the installation of a new barricade control system.

On 5 Aug 2000, the same barricade sprang up under the German Defense Minister, who -- arriving for a Pentagon honors ceremony -- was injured and briefly hospitalized, along with the German defense attache' and an American security aide. [Source: Reuters item in \*The New York Times\*, 6 Sep 2000]

[Conspiracy in Artificial Intelligence?]

---

## ✶ U.Wisconsin alters photo to add "diversity" to student body

"Peter G. Neumann" <neumann@csl.sri.com>  
*Wed, 20 Sep 2000 21:08:09 -0700 (PDT)*

The University of Wisconsin has owned up to altering a 1993 photo of a crowd of white football fans, inserting the face of a 1994 black senior in an effort to have their brochure illustrate the diversity of the student body. [Digital editing capabilities of course make such manipulations ever easier, as we have noted here many times.] (For old-time programmers, this might make the fight song "On Wisconsin" be interpreted as a PL/I ON-condition.) [Source: AP item, \*Palo Alto Daily News\*, 21 Sep 2000. See also <http://www.cnn.com/2000/US/09/20/photo.fix.ap/index.html>.]

---

## **Why software fails**

Mike Lewis <mglewis@uswest.net>

*Tuesday, September 19, 2000 6:15 PM*

As is well known, entropy is a measure of the extent to which energy can be lost in statistical systems. It appears in many equations, particularly two

$G = U - T * S$ , a thermodynamic equation, and

$S = - k * \log (p)$ , the equation used to describe the entropy of information, that is, of files.

In these,  $S$  is the entropy,  $G$  is the Gibbs Free Energy,  $T$  is temperature, and  $U$  is internal energy;  $k$  is Boltzmann's constant and  $p$  is the probability.

In systems, the semantic and philosophical and epistemological boundaries two seemingly different forms of entropy inevitably become uncertain, they overlap, and the difference gradually becomes degenerate. That's when much software fails or becomes obsolete.

Software is very complex systems and it can readily be demonstrated that a well written, strong program competing for control of hardware against a badly written program can usually get control of the machine. This happens all the time as different software designers write their very best code to get control of the processor as quickly as possible in the face of competing software from other manufacturers. In short, software is vulnerable to statistical failures as well as to outright bugs or errors in

coding, bad logic, etc. This problem is not very much discussed yet, but one supposes it will be in time.

An example might be a financial program. Ostensibly it has nothing explicitly related to thermodynamics, but the dimension of entropy appears both in software and in thermodynamics which occurs in winter in heating a house and in summer, cooling it. The financial program is required to have a sensible relation to income and expense, while the flow of enthalpy into and out from the house reverses direction each winter and summer. I have thought for a long time, after first seeing the connection, for a good example of a case in which we do not yet define how to predict just where the system will fail, and this is about the best I can propose.

I think that software's statistical entropy tends to drift around in the environment's thermodynamic entropy and this is one of the reasons why some failures are not yet completely understood--the entropy dimension is not taken explicitly into account in designing systems, except in the solid state quantum mechanics of the CPU and other chips in the machine.

Solutions to this problem will require the assumption, in early planning of the system, that eventually the software file entropy, the electron entropy of the silicon, and the environment's thermodynamic and other statistical entropy will always inevitably become indistinct, and then plan the system knowing they cannot be held absolutely distinct from the outset.

It should be noted that the word "environment" is extremely general, and includes that of the climate, as well as of the surroundings of the planet.

Also, the time scale is very general, ranging from the geological time scale of the evolution of life, to the very short durations of time found in computers. This is because thermodynamic spectra, for instance contain and are sensitive to energy-stable terms, which do not vary in time where they are involved with immediate electronic transitions in atoms and molecules.

Interesting speculations may be found on, for instance, the burning of fossil fuels to put carbon back into circulation, because early life forms--mainly plants--from which these deposits were formed, were apparently not able to measure or control the dimension of entropy. Are we recirculating all that carbon now because we can deal now with entropy? That is, though, beyond the scope of my intention here.

Mike Lewis <mglewis@uswest.net>

---

## **⚡ Filtering, censorship, silence: Who owns the language?**

Richard Schroepel <rcs@baskerville.CS.Arizona.EDU>

*Thu, 21 Sep 2000 09:16:31 -0700 (MST)*

> Subject: OPEC site hacked  
> ...  
> when I say to you guys to get your collective a\*\*es in gear  
with the crude  
> ...

> [[http://dailynews.yahoo.com/h/nm/20000913/od/website\\_dc\\_1.html](http://dailynews.yahoo.com/h/nm/20000913/od/website_dc_1.html), PGN-ed  
> with \*\* filtering]

Peter, does this mean that you've decided to accommodate to filtering software as the "lesser evil"? [See NOTE] I think this issue deserves more discussion with your audience. We probably won't be talking about b\*\*\*\*t cancer, but we've already seen too many amusing examples of filters gone am\*k.

What are the issues when persons impose communications restrictions by threatening to cutoff communications (or doing it) that don't adhere to policy? Typically the person defining the restrictions is inaccessible to reason, being buried within a large impersonal organization. Often the restrictions are a trade secret. The rejected mail gives no particular notice to either the intended recipient or the sender -- the discard is silent.

I operate a couple of "ascii text only, please" mailing lists, but it's a struggle to maintain what's become a minority format.

Most of the NIST AES documents are in PDF-only, and not readable by a text-based terminal. (From a standards organization!) The IRS tax forms and instructions aren't available as text. The instructions should be grep-able, but aren't. And so on.

This seems like a losing battle to me, but I still think a general discussion is long overdue of the consequences that follow from

"I'll only communicate in my special language." I've always assumed that the pressure was toward a common language, but the business interests of Microsoft, Adobe, IBM &c seem to operate in the other direction.

We might require by law that govt stuff be available as text (where possible), but that's only part of the larger issue: "Who controls the terms of communication?"

Rich Schroepel    rcs@cs.arizona.edu

[NOTE: Actually, no. In this case there is no lesser of weevils.

Sometimes I get many filtering bounces because I have let challenging

words go through. But I have also been assiduously informing RISKS

recipients that their filtering is stupidly overaggressive in response to

all of the bounces I receive each time I send out an issue. PGN]

---

## ⚡ Re: Decimalization and Ford Stock Splits (Carroll, [RISKS-21.05](#))

"Prodin, Timothy (T.R.)" <tprodin@ford.com>

*Thu, 21 Sep 2000 11:28:58 -0400*

On 7 Aug 2000, Ford completed its Value Enhancement Plan, a somewhat complicated stock transaction where Ford created a new company (Ford Value Company) and issued a new stock. Ford Stock holders of record on July 27th had the option of taking the new common or Class B stock plus 1) \$20 per share, 2) a fraction of the new common stock that would be the

equivalent of  
\$20, or 3) a fraction of cash and fractional shares that would  
maintain  
their percentage ownership of all outstanding shares constant.

For the last two options; the fraction of cash and fraction of  
shares  
depended on the total number of outstanding shares of the old  
company.

At the end of the exchange and disbursement; the new company  
transformed  
back into the old company; and trades on the NYSE as F.

The final numbers wound up such that if you took the full  
fractional new  
share with your matching full share; you received an additional  
0.748  
additional share.

Tim Prodin

[Also commented upon by various other readers. Many  
thanks to you all for helping correct the record. PGN]

---

## **⚡ Re: Identity theft (Ellison, [RISKS-21.05](#))**

Martin Minow <minow@pobox.com>  
*Wed, 20 Sep 2000 20:08:29 -0700*

> Now -- how do we get consumer protection laws that make it  
clear that a  
> consumer is not liable for any debts incurred by someone  
claiming to be  
> him/her ...

Having recently been on the receiving end of identity theft, I'm  
a bit more

optimistic than Carl. I solved my problem by reading the back page of the credit report, where it provided addresses of the federal agencies that regulate collection bureaus, banks, and similar organizations. Letters to the agencies resulted in one "opening a case" and, eventually, a letter of apology from the bank in question (who hadn't answered my previous requests/complaints). I used an account record book -- a bound notebook with numbered pages -- that had dated notes of every interaction I had with the banks and credit card agencies, interspersed with software notes, interesting URL's, telemarketing caller numbers, and other scribbles. This let me document my complaints with the specific dates and times that I attempted to resolve the problem.

Martin Minow minow@pobox.com

---

## **⚡ Re: Qualcomm CEO's laptop vanishes (Leshner, [RISKS-21.05](#))**

<Camillo.Sars@F-Secure.com>

*21 Sep 2000 11:43:47 +0300*

As I have some experience in the field, having lead the development of one of the tools David is referring to, I'd like to point out a few other risks associated with this issue.

Using real (and real-time!) encryption on data files does help against the threat of unauthorized information disclosure. Which is good.

But, as usual, increased security in one field can lead to increased risk in another. Encrypted files are subject to several threats.

The primary risk is threats against integrity. Tweak a bit in an encrypted file, and at least an entire block is corrupted \*). Usually the entire file can be considered lost, and a backup needs to be restored. I will not go into the discussion about how to properly encrypt backups here.

Another threat is the risk caused by loss of the encryption key. Strong encryption has the nice property that nobody can get the data without the correct key. Strong encryption has the less nice property that not even the owner of the information can get the data without the correct key. I have seen this happen. It is not a nice situation.

> It's also a message to crypto companies. Create real tools for this task,  
> ones that even C[E,F,T]O's can grok how to use {1}. A recent USENIX study  
> reported that a large percentage of users failed to use PGP correctly.

I have come to the conclusion that persons that are not trained in security must rarely or never be called upon to make security-related decisions. As Ross Anderson put it in his paper "Why Cryptosystems Fail": "...most security failures are due to implementation and management errors." I have taken to interpreting this in a very broad sense.

> {1: Getting them to follow practices is the 2nd half of the problem; as the  
> Deutch case demonstrates....}

Thus, I second Ross Anderson's view that a paradigm shift is required.

Let's not only make systems that are easier to use correctly. Let's make systems that are difficult to use incorrectly.

Camillo Sars

\*) Tweaking a bit in an encrypted file should invalidate data. If it does not, the system is vulnerable to replacement attacks. E.g. copying the encrypted salary of the CEO and pasting it over the encrypted salary on your own paycheck. Which would be nice.

Camillo Sars <Camillo.Sars@F-Secure.com> <http://www.iki.fi/ged/>

Researcher, F-Secure Corporation <http://www.F-Secure.com>

---

## **⚡ Re: Risks of using HTML Mail and HTTP proxy "censorware" together**

"J.D. Abolins" <jda-ir@pluto.njcc.com>

*Thu, 21 Sep 2000 11:02:37 -0400 (EDT)*

This risk underscores monitoring tools' user to realize that their tools have limitations. The assumption may be that a "hit" on a forbidden site means that a particular user willfully went there. Wrong, as Dan Birchall's posting shows.

I have been testing the recently reported MS Office document Web bugs to see if they can be used to rack up hits on workplace HTTP

"censorware." The tests aren't finished but here's the concept. Insert spacer gif URLs from a banned site in an "appropriate for the workplace" Word document, Excel spreadsheet, or PowerPoint presentation. When the document is opened, it should attempt to pull the graphic from the "banned" Web site and, thus, score hits on the "censorware." A document could be loaded with multiple bugs, each from a different banned site.

It is also possible to resize a URL-based image so it is hard to see. So it might not be only transparent gifs that could be (mis)used in this manner.

People investigating hits on banned sites should look for other evidence besides the "censorware" logs and not assume automatic guilt.

Beside nearly invisible graphics in the HTML e-mail, there is the risk of spoofed links. The e-mail text says the link goes to one place while the underlying HTML gives a different HREF. This has been reported elsewhere. A variant can be to use the file:// type of URL to bring up locally accessible files. Sometimes this is used as a Web joke where a visitor is convinced that the Web site can see her C: drive or /etc/passwd file. If the sender of HTML e-mail has a good idea of the systems used by the recipient, the spoofed links can be tailored to use the file:// URLs or the res:// URL.

J.D. Abolins, Meyda Online -- Infosec & Privacy Studies <http://www.meydabbs.com>

## ⚡ Artificial Intelligence strikes again

Rodger Whitlock <totototo@mail.pacificcoast.net>

*Sat, 23 Sep 2000 12:33:58 GMT*

One of our secretaries at work related an interesting tale: she and her husband went to buy gasoline, using their Visa card at the pump. It was rejected. They tried another station. Same thing. They tried to buy flowers for an aged relative. Same thing.

She phoned the issuer (Canadian Imperial Bank of Commerce - CIBC) and asked what was going on.

The response was that the computer had detected an "unusual pattern of purchases" and put a freeze on the card. The unusual pattern was the use of the card to pay a ferry fare to Vancouver and when Visa phoned to double check, there was no one home to answer the phone. Naturally: the whole family was on the ferry!

As this secretary said, what would have happened if the card got frozen after flying to Europe? Badly thought-out computer wonkism strikes again.

Regular RISKS readers probably recognize the syndrome.

Rodger Whitlock, Victoria, British Columbia, Canada

---

## ⚡ SBC Calling Card PIN

"Conrad Heiney" <conrad@fringehead.org>

*Sat, 23 Sep 2000 14:02:43 -0700*

SBC Communications, through my local telephone company (Pacific Bell) has reissued their telephone "Calling Card" telephone cards. The new cards are intended to be used worldwide and to replace previous local cards.

The card is marked with the subscriber's name and telephone number. There is also a Personal Identification Number which is provided separately, the idea being that both the telephone number and the PIN need to be present for authentication.

However, there is a space on the card for your PIN, and you are instructed to immediately write the PIN on this space so you won't forget it.

This contradicts the policy of bank ATM cards and other PIN-based systems, in which the PIN is intended to be memorized and customers are instructed in large capital letters not to write the PIN on the card or store it with the card.

The risks here are twofold:

- 1) The PIN is useless if the card is lost or stolen
- 2) Consumers will be confused by contradictory policies from different organizations and will likely write their PIN on every card they use.

Two cheers for self-sabotaging authentication systems!

Conrad Heiney conrad@fringehead.org <http://fringehead.org/>

[Several other messages relating to credit cards per se are not included here. 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 21: Issue 7**

**Sat 30 September 2000**

## Contents

- [California DMV fosters identity theft?](#)  
[PGN](#)
- [Single points of failure and backup plans](#)  
[William P.N. Smith](#)
- [Control of Olympics news coverage](#)  
[NewsScan](#)
- [Tighter security poses a security threat](#)  
[Ray Randolph](#)
- [Cochise County election computer errors](#)  
[Nicky L. Sizemore](#)
- [The risk of identity theft](#)  
[Amrith Kumar](#)
- [De Fault is in Default](#)  
[Charlie Shub](#)
- [Re: AI strikes again](#)  
[Perry Bowker](#)  
[Zygo Blaxell](#)
- [REVIEW: "CyberShock", Winn Schwartau](#)  
[Rob Slade](#)
- [Info on RISKS \(comp.risks\)](#)

## ✦ California DMV fosters identity theft?

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

*Mon, 25 Sep 2000 14:08:03 PDT*

An AP item (seen by me on the front page of the \*Palo Alto Daily News\*, 25 Sep 2000) says that the California Department of Motor Vehicles issued over 100,000 fraudulent drivers' licenses in 1999, and typically makes little or no effort to check the validity of the 900,000 duplicate license requests it receives each year. Examples include duplicate licenses issued to people of the wrong race or the wrong gender, and in one case bogus duplicates of a particular individual's license to 18 different people. The driver's license is called a ``breeding document'' for identity thieves, leading to financial fraud, ruined credit, purchases of firearms by felons, and other misuses. DMV officials claim that implementing an on-line photo-retrieval system would cost \$3 million over the next two years. This seems like a useful system -- especially if it were used pervasively.

---

## ✦ Single points of failure and backup plans

"William P.N. Smith" <wpns@compusmiths.com>

*Mon, 25 Sep 2000 17:00:37 -0400*

Last night our cable modem (currently AT&T Roadrunner, name

subject to  
change daily 8\*) stopped working, and the constant busy signals  
from  
their tech support line led me to believe it wasn't merely Yet  
Another  
Outage (TM).

Strangely, my cable modem lights were all doing the right thing,  
and  
when I checked with my neighbors, their cable modems were  
working fine.  
After a couple of hours of redialing I finally got a message  
saying that  
there were unspecified problems that they were working on  
(strange,  
usually they list the affected towns) and after some time on  
hold I  
finally talked to a tech support rep who offered to help "if I  
can".

Turns out the DHCP server for the entire northeast went down,  
and as  
people's leases on their IP addresses expired, they were dropped  
off the  
network. I asked about the secondary or backup DHCP servers, but  
apparently there was so much demand due to expired leases that  
the  
backup server couldn't respond quickly enough, and was getting  
overloaded with requests.

Risks:

Even single users ought to have a backup Internet connection  
(dialup ISP  
worked for me, but not my wife, as she has no modem...)

You know you're in trouble when your customers have your tech  
support in  
their speed dial. Customers know they are in trouble when they  
get busy  
signals on your tech support line.

Serious system-wide failures might leave some systems operating

normally  
for a while.

Your backups might have to be more powerful than your primary servers,  
or alternately customer growth might mask server deficiencies.

William Smith      wpns@compusmiths.com      N1JBJ@amsat.org  
ComputerSmiths Consulting, Inc.      www.compusmiths.com

---

## ✶ Control of Olympics news coverage

"NewsScan" <newsscan@newsscan.com>

*Mon, 25 Sep 2000 09:56:04 -0700*

Concerned that the Internet will compete with TV coverage and cut into its major source of revenue, the organizers of the 27th Olympics Games are taking a hard line about what words and images can be communicated by Internet about the sporting events now going on in Sydney, Australia. They have forbidden athlete diaries and online chats, and all streaming video (even of trial events that took place months ago. Referring to a recent lawsuit in Virginia supporting the Olympics Committee's efforts to restrict Internet coverage, constitutional lawyer Floyd Abrams thinks it's ironic that "the increased availability of a means of communication leads to a ruling seeking to assure that less is said." (\*The New York Times\*, 25 Sep 2000 <http://partners.nytimes.com/2000/09/25/technology/25WEB.html>; NewsScan Daily, 25 September 2000)

---

## ✶ Tighter security poses a security threat

"Ray Randolph" <rayr@rayrandolph.com>

Mon, 25 Sep 2000 20:35:49 -0600

Today's \*Christian Science Monitor\* online edition discusses a newly released report, the \*Baker-Hamilton Report\*, prepared at the request of the DOE. The report says in essence that scientists at Los Alamos National Weapons Labs have become afraid of reporting or admitting even minor security breaches as a result of the threat of an aggressive prosecution and in the wake of the Wen Ho Lee situation. Who can blame them? The RISKS should be fairly obvious. The entire article can be accessed at:

<http://www.christiansciencemonitor.com/durable/2000/09/26/fp2s2-csm.shtml>

A quick search for the "Baker-Hamilton report" on the DOE web site didn't turn up anything, but I would imagine that the report itself would make for fairly interesting reading for any RISK follower.

[The Government gave a terrible example of \*when holey\* prosecutions can run amok (holey, i.e., having holes). Perhaps the "situation" (as Ray calls it) will become known as an \*Un-Ho-Lee Mess\* (unholy, i.e., of questionable authority).  
PGN]

## ✶ Cochise County election computer errors

"Nicky L. Sizemore" <bolshev@theriver.com>

Thu, 28 Sep 2000 20:31:41 -0700

Cochise county, in the southwest corner of Arizona, had a primary and special election Tuesday, 12 September. In it they used a new computer tallying system obtained by the state for rural ballot counting.

Our local paper, \*The Sierra Vista Herald\*, reports that results from the elections were delayed due to software errors in the new system. According to the paper, the major errors centered around counting as major party votes those cast in nonpartisan (non-primary) positions and overcounting third-party, e.g., Libertarian, votes.

In addition to the usual issues of inadequate verification, validation, and test (VV&T), this was the first election here in which everyone could vote in a primary. Seems rash to implement a new voting protocol and a new ballot tally system in the same election.

Votes are being recounted using the old system, which was kept as a backup provision. At least they got that right.

Reporting on story from Sierra Vista Herald:

<http://www.svherald.com/news/bnews/stories/00030203bn.html>

<http://www.svherald.com/news/bnews/stories/00091301bn.html>

<http://www.svherald.com/news/stories/00091301n.html>

<http://www.svherald.com/news/bnews/stories/00091402bn.html>

[html](#)

[http://www.svherald.com/news/bnews/stories/00091501bn.](http://www.svherald.com/news/bnews/stories/00091501bn.html)

[html](#)

---

## **✶ The risk of identity theft**

Amrith Kumar <amrithk@earthlink.net>

*Fri, 29 Sep 2000 16:18:02 -0400 (EDT)*

In October 1998, the company that I worked for (let's call it A Inc) was acquired by another company (let's call it B Inc).

"A Inc" issued me a corporate credit card (from Amex) a long time before that. Around January 1999, B Inc decided that they needed to issue me a new corporate credit card ...

But, "B Inc" also wanted to spin of a portion of the acquired company and in February 1999, they created a spinoff company (let's call it C Inc).

In all this confusion, I was left with an Amex Credit card from A Inc which expired in February, I got a new Amex Credit card for C Inc in February and I was fat dumb and happy. I never quite got the Amex card from B Inc, maybe they never had it mailed out or something weird happened there; or maybe it was just lost in the mail.

But, B Inc went ahead and told our in-house Amex Travel Agency to change my travel profile to use the new credit card that they had issued for me.

In January 2000, I moved and informed Amex of my address change in regards to the card from C Inc. Then in February 2000, I made a purchase through the in-house Amex Travel Agency for a ticket for business travel. The way in which A Inc and C Inc handle business travel tickets is that Amex directly charges the corporation and no charge appears on my credit card bill.

Today, September 29th, I get a call from a collection agency indicating that an Amex card in my name, with my SSN, my correct name and my old address was delinquent and the charges were airline tickets issued in February.

After much investigation, I gathered all the information I presented above but here's where it begins to get interesting.

I have the Amex Credit Aware reporting service. That, when I started getting it in March 2000, did not list the personal Amex card that I had, the card that they were charging \$5.99 or whatever ...

Second, it did not list my corporate card (the one from A Inc or C Inc). It surely did not list the one from B Inc.

As part of all this investigation, I called Amex Fraud Investigation and they took my SSN and they showed all three cards.

I called Experian and because initially it was being handled as a fraud, they actually took my SSN and said they showed three Amex cards on my SSN. They took SSN, last name, first name, address and all that to verify that I

was in fact the person whose records they were looking at and then they confirmed the last 5 digits of all three accounts, my personal one, my corporate one from C Inc and the corporate one from B Inc

What caused this whole mixup ?

1. Your SSN is not your sole identifier for purposes of Credit, name is also significant.

2. Amex (for my personal card) had my last name and first name interchanged which is why the card would not show up on the Credit Aware Service.

3. Corporate Cards don't appear to show up on there for some reason, not sure if it's the same as 2.

4. An employer can / may apply for a card in your name, maybe without your knowledge. They reveal your name, SSN and all that nice stuff to someone.

5. When companies get bought and sold, strange things happen to these cards and the information there.

B Inc was not paying me any salary but they had an active card in my name. I called them and told the folks there in their Finance office and sure enough they had my card on file ...

6. If you have no balance on a card, you sometimes get no bill. In my case, for the four months in 1998/1999, I had no balance on the card because I never knew I had it. So I never got a statement. People move, addresses change ... the bills suddenly appear. I used to live in an apt

and mail for  
previous tenants is regular; it usually goes to the trash can.

and finally

7. I had two Amex cards that I knew of, both had valid addresses. Amex could not find me or figure out that the address was wrong when the card went delinquent. I don't believe they even contacted the company that I was supposed to work for (it was a corporate card). And yet, a collection agency could find me.

8. A credit monitoring service is somewhat questionable.

What if any is the real solution to this problem? Thankfully, my employer readily agreed to help out, the amount in question was about \$800, and I paid and will get reimbursed etc. But what's the real solution?

Amrith Kumar <amrithk@earthlink.net>

---

## **⚡ De Fault is in Default**

Charlie Shub <cdash@ludell.uccs.edu>  
*Fri, 29 Sep 2000 10:18:44 -0600 (MDT)*

My trash company bills quarterly. I would rather pay every six months.

This June, I got the \$36.00 bill and paid the \$72.00 by check.

Last week, I

got a bill for \$36.00 for the final quarter of this year.

Apparently, (if I

understood the customer-service person correctly) they use a piece of

billing software in which the amount paid defaults to the amount

owed once  
the account number is entered, and the data-entry person must manually  
override the amount if a customer remits any amount other than the default.

Fortunately, my record showed a history of paying semiannual amounts every  
six months, so the rep fixed it on the spot, taking my word that the check  
had cleared in the larger amount. His comment was to the effect that "I  
know how his software works, and I'm almost certain of what happened, so  
I'll take your word for it."

charlie shub University of Colorado at ColSpgs <http://cs.uccs.edu/~cdash>  
cdash@cs.uccs.edu -or- cdash@mail.uccs.edu (719) 262-3492

[It is unusual that Pride goeth before Default. PGN]

---

## ✦ **Re: AI strikes again (Whitlock, [RISKS-21.06](#))**

"Perry Bowker/Markham/IBM" <pbowker@ca.ibm.com>  
*Tue, 26 Sep 2000 20:36:40 -0400*

I think this is unfair to the issuing bank. I also once received a call from  
the same bank, because their computer detected that I was charging a few  
things in Toronto, and I also seemed to be in Jamaica, running up several \$K  
in cash advances! Someone had obviously captured my card number and was  
using it for all it was worth (with the apparent compliance of some Jamaican  
merchants)

Within minutes, the card was frozen, and I received a replacement by courier within 24 hours. Otherwise, it would have been weeks before I even knew this was happening, and likely many months to sort out the problem, and with a high risk of cost to me. I think it was a pretty good trade-off.

If this bothers you, better to carry two different cards, just in case, and be thankful someone is trying to protect your backside!

Perry Bowker, Toronto, Canada

[It obviously works (or doesn't work) both ways. PGN]

---

## ✉ **Re: AI strikes again (Whitlock, [RISKS-21.06](#))**

Zygo Blaxell <uryse0d5@umail.furryterror.org>  
26 Sep 2000 13:55:25 -0400

Actually, this protocol can work reasonably well if you have a cell phone. On two occasions, with two different banks (one of them was the CIBC), I've been called almost immediately after making a large purchase and challenged to recite various pieces of information from my credit application (doing that with a cell phone has its own risks, of course, which can be mitigated by phoning back using the merchant's phone).

I note that this protocol doesn't seem to stop the initial transaction from being completed. In both cases I was called some minutes after I had left

the store with my purchases.

---

## ✶REVIEW: "CyberShock", Winn Schwartau

Rob Slade <rslade@sprint.ca>

Mon, 25 Sep 2000 08:35:06 -0800

BKCBRSBK.RVW 20000625

"CyberShock", Winn Schwartau, 2000, 1-56025-246-4, U\$24.95

%A Winn Schwartau winn@infowar.com,winns@gte.net

%C Fourth Floor, 841 Broadway, New York, NY 10003

%D 2000

%G 1-56025-246-4

%I Thunder's Mouth/Inter.Pact Press

%O U\$24.95 212-780-0380 fax: 813-393-6361

%P 470 p.

%T "CyberShock: Surviving Hackers, Phreakers, Identity Thieves,  
Internet Terrorists and Weapons of Mass Disruption"

As some may know, Winn Schwartau and I do not see eye-to-eye on  
the emphasis

to be given to certain exhortations in alerting the public to  
matters of

computer security. So when he informed me of his latest book,  
he noted that

I might like to do the usual hatchet job on it. Unfortunately,  
I can't

fully comply. While I may quibble with some aspects of his  
latest book,

overall it is a good overview of the existing computer security  
situation,

and would make a helpful introduction for new computer and  
Internet users.

Part one is an outline of hackers and hacking. "The Great New  
Global  
Society" appears to be (although erudite and readable it's not  
exactly

straightforward) a presentation of society as seriously messed up, and hackers as curious and determined. The results of a number of surveys of computer penetration are described in "Whole Lotta Hacking Goin' On," with unfortunately little space given to the design of the studies. There are some examples of Web site defacement and an ad for Linux in "CyberGraffiti." (And it's attrition.org, not attrition.com.) "Who Are the Hackers?" gives a reasonable structure to the current security breaking population and environment, although, as Schwartz notes, the game has become so big and ill-defined that one might be forgiven for coming out of this chapter thinking that anyone could be a hacker and a hacker could be anyone. Some stories from the annual DefCon (and the inadequacies of the Plaza Hotel) are retailed in "CyberChrist at the Hacker Con." "Hacktivism" lists a few examples of digital civil disobedience. "An American Alien Hacks Through Customs" is probably fair warning to customs agents that if you mess with Schwartz at the border you are going to look really silly in his next book.

Part two looks into protecting you and yours. "In Cyberspace You're Guilty Until Proven Innocent" describes identity theft, and the ease and dangers thereof. (It also includes a rather odd section on Web privacy security.) The chapter admits that there is not much you can do about identity theft. It is also very US-centric: for example, the Canadian SIN (Social Insurance Number), as opposed to the US SSN (Social Security Number), is very seldom

used for commercial transactions. The advice in "Protecting Your Kids and Family From Hackers" is not an easy or quick fix, but it is (with the notable exception of the piece on cyberstalking) realistic and well written. So is the counsel in "Spam." "Scam Spam" offers very useful and relevant guidance on dealing with fraud on the net.

Part three outlines the techniques of hacking itself. "Getting Anonymous" is a quick overview of anonymizing services and spoofing. Some of the basics are skipped in "Password Hacking," but there is a nice introduction to biometric techniques. While not getting into the gritty details, there is a quick lesson on eavesdropping on promiscuous networks in "Hack and Sniff." "Scanning, Breaking and Entering" lays out the information that is--must be--available to anyone wanting to mount a network attack. "War Dialing" basically notes that phones are a means of access. Leaving aside a minor quibble with the definition of trojan horse software (like the Trojans who "installed" the horse of their own destruction because they didn't know what it contained, users generally install trojans because of a misrepresentation of what the software does), most of "Trojan Hacking" only describes Back Orifice. There is some small degree of comfort for credit card users, and some rather embarrassing points for credit card merchants, in "Hacking for \$." While it waffles a little, "Viruses, Hoaxes, and Other Animals" contains good advice and a reasonable picture of the current situation. "Crypto Hacking" is (absent an impossible IP address) a nice

history of cryptography, although it's a bit thin on details. "Steganography" defines the term, but misses a few points on usage. The discussion of computer forensics in "Hacking for Evidence" is limited to data recovery, but has some good points for users and companies.

Part four deals with destructive activities. "Denial of Service" rather overstates the point, since the term generally is restricted to operations that inhibit use but do not harm hardware or data. "Schwartau to Congress" appears to be a minor aside. The discussion of electromagnetic weaponry in "Weapons of Mass Disruption" is fascinating, but does downplay a few inconvenient laws of physics, such as inverse square distance relationships.

Part five analyses some tips for protecting yourself. "Hiring Hackers" examines both sides of the question. The basics of intrusion detection is outlined in "Catching Hackers." There is a decent introduction to firewalls in "Defensive Hacking," along with a pointer to simple automated penetration testing. "Corporate Anti-Hacking" presents a number of good points (although if you follow all of them blindly you'll likely face mass resignations). Deception is promoted in "Lying to Hackers is OK By Me."

Part six discusses law enforcement. "Hacking and Law Enforcement" is rather depressing, but reasonable. The advice on striking back boils down to "be careful" in "Corporate Vigilantism." "Infrastructure Is Us" seems to be a bit out of place, in that it presents no protective measures: only a

warning. Similarly, the material on infowar is alarming but not really illuminating in "Something Other Than War."

Part seven looks to the future. "Luddite's Lament" expresses frustration with phones. "The Future of Microsoft" is one of the standard jokes about Microsoft's fight with the US federal government. Digital manipulation of propaganda is mentioned in "Messing With the Collective Mind." "Extreme Hacking" gives short takes on some new technologies. "The Toaster Rebellion of '08" is one of the standard scifi plots.

While there is a heavy emphasis on the sensational, overall this book does provide the security novice with a fairly reliable picture of the current security environment. Possibilities are generally presented as such, and the analysis of relative dangers is usually good. A number of useful tips are given that can help home and small business computer users be more secure in their computer and network use. Security specialists will find little that is new here, but that is not the target audience for the book. I have frequently been asked for a recommendation for a general security introduction directed at the non-technical computer and Internet user, and, for all its flaws, I think this work may be the closest I've seen.

copyright Robert M. Slade, 2000    BKCBRSBK.RVW    20000625  
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 21: Issue 8**

**Weds 11 October 2000**

## Contents

- [50 million adults at risk for 'net illiteracy'](#)  
[NewsScan](#)
- [China announces new rules for Internet content](#)  
[NewsScan](#)
- [Italian police stop digital bank robbery](#)  
[Meine van der Meulen](#)
- [Computer-related sewage release into Massachusetts Bay](#)  
[Jonathan Drummey](#)
- [ISP whacks game fan with \\$24,000 bandwidth fine](#)  
[Doneel Edelson](#)
- [I've been dropped from a life-time membership](#)  
[Leonard X. Finegold](#)
- [Carnivore review team information leaked](#)  
[PGN](#)
- [What Bloatware is Not](#)  
[Rick Downes](#)
- [EMI, TWA 800 and Swissair 111](#)  
[Peter B. Ladkin](#)
- [ABC newradio network blocked during Olympics](#)  
[Phillip Musumeci](#)

- [The need for functioning IT environments](#)  
[Thomas Roessler](#)
  - [Re: Why software fails](#)  
[Jurek Kirakowski](#)
  - [Intel hasn't learned...](#)  
[Steve Bellovin](#)
  - [Test Practitioner Syllabus: 17 Oct deadline for comments](#)  
[Dorothy Graham](#)
  - [REVIEW: "Storming Heaven", Kyle Mills](#)  
[Rob Slade](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

## ✶ 50 million adults at risk for 'net illiteracy'

"NewsScan" <newsscan@newsscan.com>

Mon, 02 Oct 2000 09:23:08 -0700

As many as 50 million U.S. adults are at risk for becoming functionally illiterate in the coming years because they're technologically deprived, according to a Gartner Group study. "The Internet will soon be so pervasive that not having access to the technology or not knowing how to use it will be the equivalent of not knowing how to read or write," says Gartner CEO Michael Fleisher. The report confirms the existence of a "digital divide" that denies 65% of "lower socioeconomic-status" Americans access to the Internet, compared with only 17% in the top income bracket. But beyond simple access, a second "experience gap" separates people knowledgeable enough to tap the benefits of the Internet from those who are not. Meanwhile, a third divide is developing between those with high-

speed,  
broadband access and those stuck with straight dialup accounts.  
"As  
broadband access reaches higher penetration rates, we can expect  
to see a  
gap in broadband adoption that mirrors today's gaps in (personal  
computer)  
ownership. This will be the equivalent of having the moderate  
and upper  
classes in IMAX theaters while the underprivileged are still  
watching silent  
movies," says Fleisher. (Reuters/MSNBC 2 Oct 2000;  
<http://www.msnbc.com/news/470998.asp>; NewsScan Daily, 2 October  
2000)

---

## **✶ China announces new rules for Internet content**

"NewsScan" <[newsscan@newsscan.com](mailto:newsscan@newsscan.com)>

*Tue, 03 Oct 2000 09:46:02 -0700*

In its continuing effort to keep a lid on the impact of the  
Internet,  
China's government has issued new regulations that hold companies  
responsible for blocking illegal or subversive content, limit  
foreign  
investment, and threaten to close down any unlicensed  
operations. Internet  
content and service providers are directed to keep records of  
all content on  
their Web sites and all the users who dial into the servers for  
60 days, and  
turn those records over to police on demand. "This creates a  
system that  
would require such a scale of enforcement that it could  
potentially occupy  
the whole efforts of ICPs," says a Beijing-based Internet  
consultant.  
"Technology will respond. It will give rise to a whole new

generation of encryption techniques." (Reuters/\*Los Angeles Times\*, 3 Oct 2000, <http://www.latimes.com/business/200001003/t000093953.html>; NewsScan Daily, 3 October 2000)

---

## **Italian police stop digital bank robbery**

"Meine van der Meulen" <meine.meulen@dgp.minvenw.nl>  
*Wed, 4 Oct 2000 15:08:35 +0200*

The robbers had hacked the computer system of the Banco de Sicilia and had almost started booking more than half a milliard dollars (2 trillion lira) to other bank accounts. The Italian paper \*La Repubblica\* says the group aimed at European money designated for the regional administration of Sicily. Apparently, the group also had plans to rob the Vatican bank, the IOR. The police arrested 21 persons: Mafiosi, computer experts, and corrupt bank employees. They are charged with money laundering, attempted burglary, and connections with the Mafia. Most of them come from Palermo (Sicily). With the cooperation of employees of the bank, the group made a computer system that looks exactly like the bank's and could connect to the bank's network after closing time. Bank employees provided the necessary passwords. The police caught the bank robbers with the help of telephone taps. (Source: ANP, 4 October 2000).

Meine van der Meulen <meine.van.der.meulen@simtech.nl>

SIMTECH ENGINEERING, Rotterdam, The Netherlands,

---

## **✶ Computer-related sewage release into Massachusetts Bay**

jonathan drummey <jonathan@verytired.com>

*Mon, 09 Oct 2000 12:50:49 -0400*

Approximately 4.3 million gallons of partially treated waste water was released from the Deer Island Treatment Plant into the bay on 29 Sep 2000, the Massachusetts Water Resources Authority reported on 8 Oct 2000. The sewage had initially been treated, but had failed to receive a secondary treatment before it was accidentally sent through the outfall tunnel, stretching 9.5 miles from Deer Island. The incident is reportedly the result of a computer problem. The outfall tunnel, which is the longest in the world, was opened on 6 Sep 2000. [Source: \*The Boston Globe\*, 9 October 2000]

[Another example of garbage in, garbage out? - jonathan]

---

## **✶ ISP whacks game fan with \$24,000 bandwidth fine**

<Doneel Edelson <doneel.edelson@eulergroup.com>

*Tue, 3 Oct 2000 12:31:21 -0400*

An online gaming fan has been hit with a \$6000 invoice from Earthlink and is set to receive another, for \$24,000 -- all for posting a movie

of upcoming

Bungie X-box title Halo on his personal Web site. The movie is a copy of an Nvidia advertisement that features Halo in action, running on the 3D graphics company's hardware. The ad appeared in July 2000, and was shown at MacWorld Expo in New York. US-based Halo fan 'Cannibal Harry' picked up the ad, digitized it, and posted it on his site, in two versions: 45MB and 32MB.

The bills resulted from 62GB traffic in downloads during July, and 4500GB during September, when his monthly data limit is 500MB.

[Source: an article

by Tony Smith, <http://www.theregister.co.uk/content/1/13668.html>]

---

## **✶ I've been dropped from a life-time membership**

"Leonard X. Finegold" <L@drexel.edu>

*Tue, 03 Oct 2000 22:35:17 -0400*

Twenty-five years ago, we took out a family life-time membership in a Memorial Society (which will cremate me at dirt-cheap prices). Called 'em about something, and they said I was no longer on their list. After a moment of silent astonishment, I asked if it was because I was already dead. They said, "Not quite, O disembodied spirit". Alas, problem seemed to be a computer switch-over, and they didn't do a comparison of old and new versions. When I said that (avoiding my usual paranoia) there are probably lots of other people likewise dropped from the land of the living, the lady

sweetly said "I don't think so".

Yours in the land of the quasi-living,

Leonard X. Finegold, Physics, Drexel University (3141 Chestnut Street)

Philadelphia PA 19104 1-215-895-2740 (allow 5 rings) or (215) 895-2708

---

## ⚡ Carnivore review team information leaked

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

*Mon, 2 Oct 2000 18:16:47 PDT*

The Department of Justice apparently attempted to hide the identity of the Carnivore review team members at IITRI; however, the censored information was extracted from a pdf file with a little Adobe hacking, and the unexpurgated version appeared on cryptome.org. [Source: <http://www.wired.com/news/politics/0,1283,39102,00.html>]

[Error in domain (.org, not .com) corrected in archive copy. PGN]

---

## ⚡ What Bloatware is Not

<main@radsoft.net>

*Sun, 01 Oct 2000 07:17:17 +0000*

Years of gawking at blubber and here comes a self-proclaimed auto mechanic with a self-proclaimed no education (officially) and he says it

better than  
anyone ever has.

He calls himself "Kwanhaeng" and his first letter is here:

<http://radsoft.net/resources/rants/20000929.htm>

And here some excerpts from one of his follow-ups.

I've met a few really good computer people over the years,  
don't get to  
talk with them much, they're too busy. They remind me of a few  
good auto  
mechanics, and a few good engineers, and maybe a few savants  
in that they  
have a holistic understanding of their subject, they really  
grasp how it  
works and what it's doing energetically and dynamically. They  
aren't  
painting by the numbers, they understand it.

The oddest part is, I've made my living with my hands, and  
those are the  
only guys I can understand, unless they talk pure math, and if  
I have a  
concept to put with the symbol, I can understand that too, and  
wail with  
it.

\* \* \* \* \*

What's happening with computers is the same thing that's  
happened with  
every other aspect of the mental, technology and society.  
Nature has a  
"chaotic" order that an "organized" chaos can never  
understand. Real order  
is small, simple, elegant and beautiful. It works because that  
is what it  
is designed to do, rather than its design being dependent on a  
lot of  
other hidden motives.

\* \* \* \* \*

Unfortunately, I quit school for that reason. But I've never stopped

studying. Thanks again. Your name has a revolutionary reputation, a

computer revolution is a very good idea.

This is of course precariously close to establishing BWK's order of

things as a "natural" one, something we "savants" as Kwanhaeng would

call us of course suspected this all along. At any rate, BWK must be

proud - or at least hopefully pleased and amused.

And instead of railing at bloatware - it's still fun to do of course -

we finally have someone define what we are doing.

Which makes it easy to see, in contrast, what bloatware really is.

- It's six-year green cards where nobody really cares. About anything.

- It's doctorate programs which exist only for the corporate good.

- It's MCPs where the school guarantees you will pass sooner or later.

- It's a "naive trust in education".

Kwanhaeng has it all over the so-called "experts". In three downloads he

saw through the "showroom flash/bloatware" hoax.

I don't know where he came from, or where he's been hiding all these

years, but I sure hope he sticks around for a while. We all need him.

Rick Downes <radsoft.net> <http://radsoft.net>

---

## ✶ EMI, TWA 800 and Swissair 111

"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>

*Tue, 10 Oct 2000 20:17:33 +0200*

Elaine Scarry published an article in the New York Review of Books (NYRB) on April 19, 1998, in which she suggested that electromagnetic interference (EMI) from outside the aircraft might have contributed to the accident to TWA 800 in July 1996. She suspected in particular various military vehicles (ships and aircraft) in the area. The article was discussed in [Risks 19.64](#) (Wood), 19.65 (Thompson) and 19.66 (Ladkin), with additional comments in 19.86 (Neumann) and 19.87 (Vistica).

Scarry's 1998 hypothesis has been refuted by research carried out by NASA and included in the NTSB "docket" on TWA 800 at [www.nts.gov](http://www.nts.gov) -> aviation -> major investigations -> TWA 800 Although the ignition source for the center fuel tank (CFT) eruption has not been definitively identified, faulty wiring is the chief suspect. External EMI is not one of the identified possibilities (although bomb and missile remain in the list as "unlikely").

Ms. Scarry has published a further article in the NYRB of September 21, 2000 (noted in [Risks 21.04](#) by Fred Ballard) in which she raises the possibility of external EMI not only causing the TWA 800 catastrophe

(again), but suggests that it could have been the cause of a radio blackout in the early part of Swissair 111's flight, and also the electrical fire which led to the aircraft's crash into the ocean off Nova Scotia.

The facts are these. NASA determined that the maximum energy that could be induced in the Fuel Quantity Indication System wiring in the Center Wing Tank of TWA 800, the tank that exploded, from a dominant external emitter, is between  $1.44 \times 10^{(-10)}$  Joules and  $1.53 \times 10^{(-9)}$  Joules, depending on the FQIS wire length (NASA/TP-2000-209867, Table 3.6.4-2, p36). However, the minimum energy required to ignite the fuel-vapor mix is widely accepted as 0.2 milliJoules, that is,  $2.0 \times 10^{(-4)}$ , which is some 5 orders of magnitude larger. Even considering the other three or four contributing "dominant" emitters, one cannot get anywhere near the required amount of energy. Thus has NASA refuted Ms. Scarry's 1998 suggestion. Ms. Scarry reiterated her suggestion in the September 21, 2000 article. It is hard to see why.

The refutation for the case of Swissair 111 is a little more involved. First, the codes used for the calculation of the EM waves inside the hull of an aircraft is dependent upon the geometry of the aircraft, the position of the wire inside the aircraft, the frequency of the waves, the number and shape of the windows, and the number of modes in the cavity, according to the NASA report. So although NASA may be implored to do their calculations

again, recalculation is not just a matter of modifying the numbers already obtained. This is for roughly the following reason.

There are nodes in the resonant waveforms inside an aircraft hull that could contain high-intensity radiation (over tiny distances of course) and maybe such a node could lie over a damaged part of a wiring bundle with two exposed conductors and cause a spark. Whether a spark is caused depends on the field intensity in the area, which is dependent mainly on the air pressure. The required intensity is about 30 kilovolts per centimeter (kV/cm) at sea level and varies roughly linearly with air pressure at lower altitudes, which means roughly 15 kV/cm at 15,000 ft, where the atmospheric pressure is about half that at sea level. This is 1.5 million volts per meter (V/m), to be compared with the field intensities of between 3.773 V/m and 32.713 V/m available to the outside of the hull of TWA 800. Although these orders of magnitude are radically different, we can't rule out arcing without running the codes. However, we can ask whether such a spark could contain enough energy for long enough time to start the insulation burning.

Patricia Cahill of the FAA performed arcing tests on aircraft wiring in 1988, 1989 and 1995. In the 1995 tests, she ran current into wiring, specially prepared to form a short circuit at the ends, from an 18.75kVA generator through standard 7.5A circuit breakers, until the insulation degraded sufficiently to catch fire. In the worst case, with aromatic

polyimide insulation (Kapton(TM)), the insulation caught fire very quickly under the load; but even in this case, most circuit breakers tripped at least once and were reset before the fire was observed to take hold.

Ms. Cahill did not attempt to measure the total energy required for the fire event, but we can estimate a lower bound from this information, knowing how much energy is required at a minimum to trip a circuit breaker (which is based on a bimetallic strip which bends with heat and trips a switch). So we obtain some figure for the minimal energy required, although by general reckoning it is too low. Never mind, it plays the required role.

This much energy must be available from EM fields outside the aircraft in order for it to be available inside the aircraft. It turns out to be a factor of 6.8 million times higher than that available on the outside of TWA 800 from the most significant emitter. And none of the emitters in the region of TWA 800 were known to be anywhere within the region of Swissair 111. A land-based emitter capable of creating this kind of field in the region of the route of flight of Swissair 111 is out of the question. Moreover, if the code results for TWA 800 are anything to go by, this energy estimate could well be orders of magnitude too low. We consider this result to refute the proposal of Ms. Scarry that external EMI could have caused the wiring fire in Swissair 111.

Connecting total energy available with a wiring fire assumes that the energy is provided to the aircraft and wiring over a specific short time frame

(noted by Hal Lewis). Energy per time unit is power, and thus not only a required total amount of energy but a required minimum power must also be present. We made no attempt to obtain a lower bound for the power.

A paper laying out this argument in more detail with references, and summarising the NASA results relevant to the refutation, is available in PDF or Postscript format at

ww.rvs.uni-bielefeld.de -> Publications -> What's New ->  
"EMI, TWA 800 and Swissair 111"

Partly as a result of these two accidents, defective wiring has become a major theme in aircraft safety investigations over the last few years.

Older aircraft such as the B747-100 involved in the TWA 800 accident have about 150 miles or so of the stuff. More modern aircraft have more electronics and more wiring, and sometime they will be getting old too. The possibility of arcing is a major area of concern. Various companies have developed so-called arc fault detection technology, which consists of a set of algorithms to recognise the electrical characteristics in the wire of an arcing event somewhere in the circuit. The major problem is to distinguish arcing from other events such as the waveform profile when motors or other loads are turned on. Such arc fault detection technology has been developed by companies such as Eaton Corp in the US, Square D/Groupe Schneider (primarily for domestic use, I understand), and ETA Technologies in Germany. ETA has recently given evidence before Congress on these matters. They hope to develop arc fault breakers with which

commercial

aircraft may be retrofitted. Let us all hope that they succeed.

The first author wishes to acknowledge the contributions to this inquiry of

William Sells and Peter Meckler of ETA Technologies, Pat Cahill of the FAA,

and Hal Lewis, emeritus of UC Santa Barbara, as well as other colleagues

obliged to remain anonymous for professional reasons.

Peter Ladkin, Faculty of Technology

Willi Schepper, Faculty of Physics

University of Bielefeld, Germany

---

## **ABC newsradio network blocked during Olympics**

Phillip Musumeci <phillip@pm.cse.rmit.EDU.AU>

*Sun, 1 Oct 2000 14:26:21 +1100 (EST)*

The Australian Broadcasting Corporation is the national broadcaster of

Australia. It uses innovative digital audio systems in-house and supplies

streaming audio feeds of its major networks' programs. During the Olympics,

its newsradio network has had its streaming audio broadcast cut in order to

comply with the Olympic organisers' arrangements for the sale of coverage.

So, in addition to the Olympics organisation scanning Internet sites for

diaries and chats ([RISKS-21.07](#)), Australians have had a 16-day black out on

one of their ABC networks streaming audio feeds.

## ✶ The need for functioning IT environments

Thomas Roessler <roessler@does-not-exist.org>

Tue, 3 Oct 2000 14:39:52 +0200

Frequently, you read about the importance of policies, version control, and so on for corporate IT security and management.

But you also regularly read about corporations finding huge amounts of pirated software on employees' PCs, and about employees not adhering to policies, eventually endangering a corporation's IT security as a whole.

One of the reasons for this kind of misbehaviour may lie in the lack of ease of use and functionality with "official" IT environments, combined with the ease of "administration" with PCs running single-user operating systems.

When users have easy access to Web mail systems, but the internal mail system happens to work flawlessly only on an occasional basis, don't be too astonished if your employees start to discuss confidential internal issues through Yahoo! and Hotmail.

When the official e-mail system doesn't work reliably and timely for external messages (or has an interface which is worse than Hotmail), don't be astonished if your employees give out private e-mail addresses to customers. "If you want to get through quickly and reliably, use ...@hotmail.com. It's not official, but it works."

When customers send messages in the Office format of the day, and employees can't read them, don't be astonished if you happen to find pirated copies of the latest releases of the software in question on their computers.

So, when thinking about security, always keep in mind that you need an environment that works well enough to be accepted by your users. If it isn't accepted, they'll sooner or later find ways to work around it, and around all your nicely-established policies and procedures. (And you don't want to spend your time on securing an environment which isn't really used, right?)

I'd hope that I've spent some 40 lines stating the obvious. However, in reality, all of what I'm describing happens on a daily basis. Just look.

---

## **✶ Re: Why software fails (Lewis, [RISKS-21.06](#))**

jk <jzk@ucc.ie>

*Thu, 05 Oct 2000 11:28:18 +0100*

Mike Lewis' piece on entropy in computer systems is a good start but he fails to take into account the human factor in designing these systems. I believe it was Fred Brooks who first pointed out that the more people fiddle with a computer program, the more likely it is to disintegrate.

The real entropy risk is computer programs which undergo

development over  
many years by different hands and under different managers.  
Remember all  
those legacy systems we used to know and love? That's how they  
got to that  
state.

When some body retains overall control of the revision process  
as for  
instance with Linux, or open-source encryption systems, the  
opposite effect  
seems to occur: perhaps an equivalent to Maxwell's daemon, who  
actually  
reverses entropy by an act of intelligence?

In the Human-Computer Interaction field, the biggest entropy  
risk is when a  
system is endlessly tweaked to make it more 'usable'/'suitable  
to users  
needs.' Unless there is exceptionally strong project management  
(which  
there rarely is) the result is the usual bloatware verging on  
chaos which  
serves nobody at all.

Jurek Kirakowski, HFRG, Ireland <http://hfrg.ucc.ie/> <http://hfrg.ucc.ie/jk/>

---

## **⚡ Intel hasn't learned...**

Steve Bellovin <[smb@research.att.com](mailto:smb@research.att.com)>  
*Mon, 02 Oct 2000 23:16:09 -0400*

An AP review describes a new Intel product aimed at children:  
the "Play  
Computer Sound Morpher". It's a microphone plus software to  
change the  
recorded voices. It also lets you "save the soun creations and

to e-mail

them to someone as an executable file with both the message and a player."

The next sentence of the review started with "A word of caution", but

it was warning of the file size, rather than the habit (and consequences) of e-mailing executables.

-Steve Bellovin

---

## ✈ **Test Practitioner Syllabus: 17 Oct deadline for comments**

Dorothy Graham <Dorothy@grove.co.uk>

*Wed, 4 Oct 2000 22:39:30 +0100*

Risk: teaching testers the wrong things, not teaching the right things?

You may be aware of the new qualifications for software testers that are being developed in the UK. The Foundation Certificate, based on a 1-hour multiple-choice exam has been very successful in its first 2 years.

The next level proposed is the Practitioner Certificate, based on a 3-hour essay exam.

The committee developing this syllabus is eager to have comments about the syllabus from test experts and practitioners, before it is "officially" published as the basis for the qualification.

They would be very grateful if you could take time to look through the syllabus and feed back your reactions and comments.

As you will see from the first page, comments need to be with Sarah Dyer by the 17th of October, less than two weeks from today. If you could choose perhaps one section of the syllabus that you are particularly interested in, that would be very helpful (and more would be even more helpful!) (For random selection, choose the one corresponding to the current last digit of your nearest digital clock.) Section 4 is on risk and testing.

Download the pdf file from: <http://www.bcs.org.uk/iseb/syll/pract.htm>

(Note that ISEB seem to be having trouble putting the right file on the web site - it is NOT the August 1999 version, but a pdf file dated 19 Sept 2000.)

If you can help, thank you very much! If not, perhaps you could ask someone else in your organisation to comment? Please forward this to anyone you know who would be interested in commenting - since time is so short, please do it now!

Dorothy Graham, Grove Consultants, Grove House, 40 Ryles Park Road,  
Macclesfield, Cheshire SK11 8AH UK Tel: 01625 616279 [www.grove.co.uk](http://www.grove.co.uk)

---

## **⚡ REVIEW: "Storming Heaven", Kyle Mills**

Rob Slade <[rslade@sprint.ca](mailto:rslade@sprint.ca)>  
*Tue, 10 Oct 2000 12:49:25 -0800*

BKSTMHVN.RVW 20000630

"Storming Heaven", Kyle Mills, 1998, 0-06-101251-3

%A Kyle Mills

%C 10 East 53rd Street, New York, NY 10022-5299

%D 1998

%G 0-06-101251-3

%I HarperCollins/Basic Books

%O 800-242-7737 fax: 212-207-7433 information@harpercollins.com

%P 499 p.

%T "Storming Heaven"

Mills can stand with the front ranks of thriller authors. His plotting is nicely developed, and realistic. (You've got to admire his bravery in taking on a very thinly disguised Scientology.) The characters are sympathetic, and quirky enough to be interesting.

What gets him into this series is a very nice use of telecommunications and security. First off, we have a great idea for eavesdropping, a long distance company that taps into all the calls made on its cards. The use of voice over IP allows you to route all calls into your processing centre, although the use of an 800 number would probably have worked just as well. (On the other hand, the use of voice over IP also allows you to justify, and hide, masses of voice processing equipment.) Offering special rates to law enforcement agencies, government offices, and legislators selects a fairly influential group to blackmail or keep track of.

Then we have identity theft and manipulation. The details of this section are not as prolific as those in the long distance plot, but, assuming the

personnel placement suggested in the book, it is all too plausible. Fairly realistically, the standard attacks on the bank accounts of the protagonist, and the production of a criminal record, are not serious threats, but are used as annoyances to add to the other assaults being used. It is also nice to see the use of social engineering, which is simpler and generally just as effective, instead of some impossible dominance over all computer systems.

The good guys use social engineering to good effect as well, although I suspect that the steps taken were really surplus to requirements. Still the penetration of the bad guys' systems is accomplished in a practical manner.

There is even a nice use of private phone exchanges, and a good way to get around the security there.

copyright Robert M. Slade, 2000    BKSTMHVN.RVW    20000630  
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 21: Issue 9**

**Friday 3 November 2000**

## Contents

- [Air-traffic control woes](#)  
[PGN](#)
- [Aviation near-crashes in Kathmandu](#)  
[Phil Carmody](#)
- [Typo + "strange glitch" = private files world-readable](#)  
[Michael Froomkin](#)
- [Risks of an 'uninterruptible power supply'](#)  
[Ross Anderson](#)
- [How to upset your customers](#)  
[John Pettitt](#)
- [Did I \\*really\\* request my password in plaintext?](#)  
[Matt Stupple](#)
- [Over capacity @Home](#)  
[Dave Isaacs](#)
- [Minister racks up \\$50,000 phone bill](#)  
[Fergus Henderson](#)
- [EZ-Pass discovers risk of sending URLs instead of actual text](#)  
[danny burstein](#)
- [Yet another daylight savings time problem...](#)  
[Gordon Henderson](#)

- [I'm falling back, and I can't get up.](#)  
[Richard Glover](#)
  - [Worm risk multiplier](#)  
[Jeremy](#)
  - [Re: Carnivore review team information leaked](#)  
[Rob Warnock](#)
  - [Re: AI strikes again](#)  
[Chris Meadows](#)  
[Marcos](#)
  - [Re: U. Wisc altered photographs: They're not the only ones](#)  
[Fredric L. Rice](#)
  - [Re: 50 million adults at risk for `net illiteracy'](#)  
[K Parker](#)
  - [CFP: Risk Assessment & Policy Assoc. International Conference](#)  
[John M. Gleason](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

## ✈ Air-traffic control woes

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

*Thu, 2 Nov 2000 17:57:09 PST*

On 19 Oct 2000, hundreds of flights were grounded or delayed because of a software problem in the Los Angeles air-traffic control system. The cause was attributed to a controller in Mexico typing 9 (instead of 5) characters of flight-description data, resulting in a buffer overflow.

On 23 Oct 2000, a computer glitch in the regional center in Fremont, California, resulted in the loss of all flight plans for northern California and western Nevada; the system failed to work following maintenance the night before.

As a result, the Federal Aviation Administration has suspended the installation of new software upgrades in ATC systems, until further notice.

[Sources: A variety of news items from diverse sources]  
[Slight correction in archive copy.]

---

## ✈ Aviation near-crashes in Kathmandu

<Ext-Phil.Carmody@nokia.com>  
*Thu, 12 Oct 2000 16:20:18 +0300*

In the space of a week:

Kathmandu, early Oct 2000: a Royal Nepal Airlines plane was hit by a vulture, the engine caught fire and was forced to return to Kathmandu.

Kathmandu, 9 Oct 2000: an Indian Airlines Airbus-300 made a successful emergency landing at Kathmandu International Airport one minute after takeoff. The right engine of the aircraft caught fire one minute after takeoff

Kathmandu, 10 Oct: Kathmandu International Airport was closed indefinitely Tuesday morning after a Boeing 757 of China South West Airlines on a flight to Lhasa probably hit a bird and the pilot braked and stopped the aircraft a few feet short of the southern end of the runway before takeoff, airport officials said.

Kathmandu, 12 Oct: Lauda Airlines Boeing 767 landed safely at Kathmandu's Tribhuvan International Airport after being hit by a vulture while landing at the airport on a flight from Vienna Thursday, travel agents and airport authorities said.

So, that's 4 incidents that have put at risk the lives of hundreds of passengers in the space of one week. Kathmandu is a particularly hazardous airport due to the fact that planes have to climb very quickly to escape from a valley. It's also slightly unfortunate from a purely sanitary point of view -- the reason there are so many birds, in particular large ones which endanger the flightworthiness of planes is because of the large landfill sites near the airport. Anecdotally (from the same source as the above, but I couldn't verify this), an emergency hunting crew has been out shooting birds in the last few days; obviously they didn't shoot enough.

No fly-by-wire, no HERO, just good old-fashioned bird-meets-engine.

Phil Carmody

[This week's Singapore 006 accident is another low-tech example for

RISKS: The plane that crashed into heavy equipment on the runway was

attempting to take off on the wrong runway! PGN]

---

**✶ Typo + "strange glitch" = private files world-readable**

"Michael Froomkin - U.Miami School of Law" <froomkin@law.miami.edu>

Wed, 1 Nov 2000 10:47:46 -0500 (EST)

The \*Miami Herald\* reports (1 Nov 2000) that "A Miami man's [Jerry Haygood] spelling mistake during an Internet search led him to sensitive e-mail messages sent to state government officials that had been inadvertently left for public view on a state Department of Health website." The information included a letter from an HIV patient seeking a doctor and other sensitive medical documents.

Mr. Haygood apparently typed "liscence" into a Dept. of Health search window. As the Herald reports [with my bracketed addition], One of the files that popped into the list of search results was a list of questions or comments e-mailed to the [www.myflorida.com] site. Most bore the sender's name, address, phone number and e-mail address. Roy Cales, the state's information technology chief, said Tuesday that Haygood's misspelling set off `a strange glitch . . . in the code that triggered the access' to what should have been a private section of the Health Department computer. As of late Tuesday, no one was sure exactly what triggered the glitch or whether a similar error could allow access to other areas thought to be private.

"`All we can say is that we are really sorry,' Cales said, `and that we will do whatever it takes'' to prevent a reoccurrence.'"

A. Michael Froomkin, Professor of Law, U. Miami School of Law,  
Coral Gables FL

33124 USA 1-305-284-4285 Please visit <http://www.icannwatch.>

[org](#)

---

## ⚡ Risks of an `uninterruptible power supply'

Ross Anderson <Ross.Anderson@cl.cam.ac.uk>

Thu, 12 Oct 2000 18:23:23 +0100

British newspapers today reported that a baby was born at Eastbourne General Hospital by Caesarian section, the operation being performed under torchlight following a power cut caused by a storm. On one account, the standby generators couldn't be started as the computer that controlled them believed they were already on; and when mains power was restored after twenty minutes it could not be switched through to the operating theatre as the computer believed that the generators were still running. On another account, the computer refused to believe that the power had gone off in the first place. [http://www.guardian.co.uk/uk\\_news/story/0,3604,381054,00.html](http://www.guardian.co.uk/uk_news/story/0,3604,381054,00.html)

The emergency lights above the operating table were not powerful enough for the doctor to work safely, so he sent nurses running to get torches from wherever they could. The nurses held the torches over the patient's abdomen in shifts to prevent their arms becoming stiff.

According to the \*Guardian\*, the operation succeeded because the patient required only a local anaesthetic and because the obstetrician had worked

for ten years in Africa. He was used to operating not just under torchlight but under candlelight. According to the 'Telegraph', there was also a heart patient who died in an ambulance outside where paramedics were trying to revive him. The hospital denied that the power cut was a contributory factor in his death.

RISKS readers will recognize a number of too-common failings such as the lack of easily usable manual overrides and a failure to test fallback modes of operation properly. Above all there seems to have been a violation of the KISS principle. As Christopher Strachey said, 'It's impossible to foresee the consequences of being clever'. Clever failsafe mechanisms should be avoided. Ross Anderson

---

## **✶ How to upset your customers**

John Pettitt <jpp@cloudview.com>  
*Mon, 16 Oct 2000 13:12:31 -0700*

There is a product call WinU (<http://www.bardon.com/winu.htm>) that "locks" windows and supposedly keeps users from doing things they shouldn't. Leaving aside the practicality of actually making such a product work the people who wrote WinU have a bigger problem.

On the web site they publish a quite extensive list of customers including any number of banks, CNN, numerous police and fire agencies etc

(<http://www.bardon.com/userlist.htm>). Well the inevitable happened:

Somebody who signs their messages "Nu Omega Tau" posted to BUGTRAQ a list of the built in "emergency passwords" (it turns out the passwords are visible as plain text in the binary).

So here we have a well publicized list of companies running what is now effectively useless security software.

---

## ⚡ Did I \*really\* request my password in plaintext?

Matt Stupple <matts@tibcofinance.com>

*Mon, 2 Oct 2000 12:33:08 -0700 (Pacific Daylight Time)*

Having recently installed the new Mac OSX Beta, I was trying to search for known bugs and fixes on the Apple website. Before I was allowed to access some part of their website I needed to enter my Apple ID (I must have registered at some point in dim and distant past) and I either entered my password incorrectly or clicked on the 'forgot my password link' ... anyway, I logged in successfully in the end and thought nothing more of it until I checked my e-mail this morning and found this message:

```
> From: AppleID@apple.com
> Subject: Your Apple ID Information
> Date: Sun, 1 Oct 2000 18:45:57 GMT
>
> As you requested, here is your Apple ID information:
>
> Apple ID : <this is actually just my e-mail address>
```

> Password : <yup, my password in plain text>  
>  
> Thank you for your interest in Apple and its products.

Need I say more?

---

## **Over capacity @Home**

Dave Isaacs <dave.isaacs@entrust.com>

*Wed, 18 Oct 2000 10:03:44 -0400*

Customers of Rogers@Home, which is affiliated with Excite@Home, have reported serious degradation in performance and reliability of their cable Internet access over the past weeks. As a Rogers@Home subscriber, I can attest to the fact that the performance has plummeted.

<http://www.globetechnology.com/archive/gam/News/20001018/ROGER.html>

<http://www.ottawacitizen.com/hightech/001018/4706091.html>

This seems to be a case of subscribing more customers than your infrastructure can handle. Didn't AOL go through this a few years back? So much for learning from the mistakes of others. I also suspect that part of the problem can be attributed to improperly merging the Rogers@Home and Excite@Home infrastructures (read: bad planning). For me, service was fine up until Rogers rolled out the new service available from their affiliation with Excite. Then performance took a nosedive.

## ⚡ Minister racks up \$50,000 phone bill

Fergus Henderson <fjh@cs.mu.OZ.AU>

12 Oct 2000 07:08:20 GMT

The opposition has demanded the resignation of Peter Reith, a senior minister in the Australian government, after it was revealed that his taxpayer-funded telephone card had accumulated a bill of \$50,000.

Details below are excerpted from a report in The Age newspaper <<http://www.theage.com.au/news/20001011/A43199-2000Oct10.html>>.

| Mr Reith admitted he wrongly gave his eldest son Paul the pin number

| of the card. He said he had repaid the estimated \$950 worth of calls

| made by his son. Official guidelines state that only MPs are allowed

| to use the card, which is issued for parliamentary and electoral use.

| It was also revealed that 11,000 calls had subsequently been made on

| the card from 900 locations, including Finland, Britain, the United

| States, Singapore, Malaysia, Hong Kong, Thailand and China.

| Mr Reith said he did not know who had made the disputed calls and that

| he had not used the card since 1994. He said he was not made aware of

| the excessive use of his card - which can be used only with a secret

| pin number - until August last year.

| "Obviously this card has fallen into the wrong hands, as it were, and

| there was unauthorised use," he said.

According to a radio report, in order to make phone calls billed to the card, you only need to know the 8-digit card number and the 4-digit pin number. The Age quoted an IT expert as saying that "telecards were easy to abuse and security was virtually non-existent."

Fergus Henderson <fjh@cs.mu.oz.au> <<http://www.cs.mu.oz.au/~fjh>>

---

## ✦ EZ-Pass discovers risk of sending URLs instead of actual text

danny burstein <dannyb@panix.com>  
*Tue, 24 Oct 2000 11:19:44 -0400 (EDT)*

In a story datelined 24-Oct-2000, and headlined:

New Jersey shuts down E-ZPass statement site after security breached

The Associated Press reported on a problem with privacy and security on the New Jersey EZPASS website where people can review their usage.

(EZPass is a radio transponder placed in your motor vehicle which is

"read" at toll booths, enabling you to zip through without having to stop

and hand over cash. Naturally it keeps records of when and where you

were for billing purposes... Which is another RISK all together)

Per the story:

TRENTON, N.J. (AP) -- A security breach has forced New Jersey officials to temporarily shut down a service that allows E-ZPass users to get monthly statements via e-mail.

The story contains claims and counter-claims, some of which are mutually exclusive, but then has the following paragraph:

Reagoso said Monday that it wasn't hard to break into the system. He discovered that the electronic statements aren't sent directly to drivers via e-mail, but rather drivers are provided with a link to access their accounts.

Presumably the link for, say, October would have been something like

www.[the number of your account].200010.[somelocation]

and all you'd have to do is replace your own account number with the person's you were looking for.

Quoting one more paragraph from the story:

"It's something that an eighth-grader who designs his own Web page at home is capable of doing," Reagoso said. "It took four accidental keystrokes to display anybody's account."

I just checked the EZPass website ([www.ezpass.com](http://www.ezpass.com)) and they don't have any comments posted...

[It turns out Mr. Reagoso has his own website:

<http://www.reagoso.com>

in which he says a bit more. DB]

---

**⚡ Yet another daylight savings time problem...**

Gordon Henderson <gordon@drogon.net>

Sun, 29 Oct 2000 14:08:36 +0000 (GMT)

Although this one is of my own doing and in a game I wrote, so it wasn't exactly critical, but I'll post the details of how easy it is to get something fundamentally wrong!

I wrote a MUD (Multi User Dungeon) game some years back. I based it on some existing code and heavily modified it. One of the things I added was the ability to execute commands on a timed basis. I needed this for various reasons to make the game work. I have a file which contains the commands and the times they execute. There are 2 types of commands - those which are executed regularly (say every 10 seconds) and those that are executed once a day at a set time.

Once a day, the game has to shutdown and reboot and this is handled by a shell script wrapper which runs the game and a shutdown command run on a timed basis from inside the game.

My timer code reads and parses the file and builds up a list of actions.

What it does is it takes the time the command needs to be executed and adds it to the current time (in seconds, Unix time(2) function) then when "now" is  $\geq$  the time the command needs to be executed, the command is executed.

So the game boots at 9:01 AM, reads it's files, the timed command file, etc. Sees a command that says that at 09:00 AM it has to execute the

shutdown command. It calculates the number of seconds from 'now' to 'then', stores this in it's file and gets on with whatever else it has to do. 86399 seconds later, it executes the shutdown command. Great, but on the 29th of October when the clocks went back an hour, this was really 08:00 AM according to the wall-clock which had been adjusted correctly as is the way it's supposed to work in the Unix world. The game rebooted, read in all it's files, saw that one of the timed commands was to shutdown at 09:00 AM, computed that this was in an hours time and carried on. One hour later it shutdown and started again.

As I mentioned earlier, this is just a game, so in reality the consequences aren't exactly dire for anyone except the odd player who was connected at that time saw a double reboot when least expecting it. It's probably never noticed in the springtime, as who's really about to notice it reboot an hour later than normal? (according to the clock on the wall)

The RISK is obviously not thinking about daylight savings time when the code was written, or maybe thinking "it's just a game", but the really bizarre thing to all this is the fact that I wrote this code some 8 years ago and no-one until now has noticed it!

Gordon <http://www.drogon.net/>

---

**⚡ I'm falling back, and I can't get up.**

Richard Glover <rglover@lunarpoodle.com>

Sun, 29 Oct 2000 13:47:46 -0800

'Tis the time of year(!) when we diddle with the clocks in the US. As part of the process of "falling back," I decided to let my mac (running OS 9.04) do this through a time server. The "Date & Time" (version 8.2) control panel has a nice feature to select a time zone, and there are are two check boxes: "Set daylight saving time automatically" and "Daylight saving time is in effect." The latter seems obvious-there are some parts of the various time zones that do not recognize DST by local custom or law. Since I live in Seattle, I checked the former "set automatically" option.

Of all the clocks in the house that should have been "correct" this morning, I would think my mac would have been it. ("Falling back" is to be done at 2:00am, allowing one to live that hour twice, but I always go around on Sunday and rest the clocks. Except my VCR, of course, which always flashes 12:00 for reasons you don't want to know.) The control panel also has a nice option to update the time on the local computer clock automatically. So, dammit, why isn't the computer clock resetting when the computer is allowed access to the time server?

Some experimentation revealed the answer. Unchecking both boxes on the control panel results in a correctly set clock to PST. (Another option I selected allows the clock to update when the computer time differs from the time server time.) Hmmm...why in the world would it work that

way? A stroke  
from Obviousman makes me recognize a risk: the checkbox indeed  
says "Set  
daylight saving time automatically." It doesn't say "synchronize  
with  
daylight saving time automatically." I suspect (but haven't  
confirmed) that  
it indeed works just like that: it will \*set\* DST in March, but  
will not  
\*unset\* it in October.

The risks are amusing:

1. "Setting" and "synchronizing" are not synonymous terms, and  
even  
when you know the difference, you shouldn't assume you know  
which was  
intended by the user. (In this case, the choice of word was  
correct,  
but why anyone would design software to work like that is beyond  
me.)
2. An option to do something "automatically" can seldom be  
trusted to  
do what you think it will when the time (!) comes.

rglover@lunarpoodle.com

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

---

## ✶ Worm risk multiplier

"Jeremy" <jeremy@electrosilk.net>  
*Tue, 17 Oct 2000 20:59:41 +0800*

I manage a number of networks and routinely review the  
penetration attempts  
from external sources. It has become apparent that there is a  
significant  
number of personal computer systems 'out there' that have been

compromised  
by a virus or worm and are now attempting to compromise other  
systems,  
including those under my control.

This observation has been triggered by an order of magnitude  
increase in  
netbios probes in the past month. presumably from a new  
variation on a  
netbios worm or virus.

The fact that a large number of external systems have been  
compromised is  
interesting, and also that these systems are trying to exploit  
mine is also  
interesting. However, the most interesting thing about this rash  
of virus  
driven exploits is that it make the compromised machines many  
times more  
visible than they might otherwise have been.

My logic is that if I have had an exploit attempt against me,  
then the  
exploiter is vulnerable. A simple log and a script can then do  
their worst,  
from simply planting a new worm/virus, through to destroying the  
attacking  
machine.

The risk is simple. An attacking worm or virus, even though  
benign, can  
trigger a much worse outcome for the attacker from a counter-  
measure hosted  
on an attacked system.

I expect that there will shortly be three classes of counter-  
measures  
created to exploit any highly visible worm/virus.

1. A sterilising counter-measure that destroys the infection on  
the  
attacking machine
2. A benign counter-measure that infects an attacking machine

with a  
different virus/worm and lets it carry on  
3. A destructive counter-measure that simply destroys the  
machine that is  
attacking

A secondary, but perhaps more interesting outcome is that  
infected machines  
advertise themselves with great vigour. This means that if your  
machine is  
infected with one of the current worms then you not only have  
the problem of  
unwanted software running on your system, but you have a bright  
beacon  
flashing over your computer saying 'come here and read all my  
information,  
because I have no security running'. From an estimation of  
damage that  
could be caused, financially or otherwise, I expect that the  
advertising  
will be far more damaging than any trivial loss of computer or  
service

Jeremy

---

## **✶ Re: Carnivore review team information leaked (PGN, [RISKS-21.08](#))**

Rob Warnock <rpw3@rigden.engr.sgi.com>

*Wed, 11 Oct 2000 19:51:44 -0700 (PDT)*

> [DOJ] attempted to hide the identity of the Carnivore review  
team  
> members at IITRI; however, the censored information was  
extracted  
> from a pdf file with a little Adobe hacking...

Actually, turns out you don't need very much hacking at all.

Simply open the document in "acroread", select any of the blacked-out text, and paste it somewhere else. Presto, change-o!! Instant cleartext.

It seems that the black bars are images, and in "acroread" images and text can be "selected" separately! (\*sigh\*)

[Error in [RISKS-21.08](#): Correct URL is <http://cryptome.org/carnivore-mask.htm>  
Will be corrected in archive copies. PGN]

---

## 🔥 Re: AI strikes again (Bowker, [RISKS-21.07](#))

Chris Meadows <robotech@eyrie.org>  
*Mon, 2 Oct 2000 12:37:41 -0500*

At the risk of possible redundancy, I have to agree with Mr. Bowker's comments in [RISKS-21.07](#). I have some firsthand experience from the other side of things, being a part-time K-Mart cashier to help support myself through college.

Declined cards happen from time to time at my store, as do "call supervisor" notices -- which means we have to call the credit-card company for authorization before we can accept it. It's a fairly simple process either way, and only takes about five minutes--and in every case that I remember, was amicably resolved so that the customer could pay for his purchase and be on his way. It held up the line, yes, but that's why our K-Mart has fourteen check-out lanes; we just call someone in from the floor

and open  
another.

Mr. Whitlock's story about the woman at multiple gas pumps was amusing for the apparent lack of common sense on the part of the credit-card people (yes, if they're on a ferry, of course they aren't home), but I'm sure it's a standard procedure they have to follow uniformly for all incidents, and they don't have any say in the matter. That's why they put the phone number on the back of the card--so people can make contact from wherever they are when their card is rejected.

As annoying as it is at times when your credit card is declined, let us not forget that this is the best way they've come up with so far to manage the risk of your card being stolen--and they do have incentive, because the credit-card people are the ones who have to eat the losses caused by fraudulent spending sprees. Getting upset over this makes about as much sense as getting upset when the cashier needs to compare the signature on your card--but there are people who have a hissy fit at either one. (And I will not even go into the people who think they're being clever not to sign anything to their cards, despite the fact that this lets the next person to find it sign his own name to it and go on a spending spree.) To paraphrase a proverb, human stupidity is the root of all risks.

Speaking for myself, I have made it part of my travel preparation routine to phone my credit-card vendors and let them know where and when I will be

traveling so they can flag it in their computers. Saves on embarrassment later on.

Chris Meadows [robotech@eyrie.org](mailto:robotech@eyrie.org) <URL:<http://www.eyrie.org/~robotech/>>

Themestream Writings: <URL:<http://www.themestream.com/articles/151255.html>>

---

## **⚡ Re: AI strikes again (Blaxell, [RISKS-21.07](#))**

<marcos@panix.com>

*Tue, 10 Oct 2000 11:52:26 -0400 (EDT)*

I am under the impression that it is a bad idea to reveal any information of the type that might be on a credit application (i.e., the Canadian equiv. of SSN, address, mother's maiden name, ...) to someone who calls you since you have no way of verifying they are who they say they are. The knowledge that just made a purchase at a certain store isn't sufficient; it could be an accomplice of an employee of the merchant.

As you say, the risk can be mitigated by phoning back using the merchant's phone.

---

## **⚡ Re: U. Wisc altered photographs: They're not the only ones**

"Fredric L. Rice" <[frice@SkepticTank.ORG](mailto:frice@SkepticTank.ORG)>

*Tue, 10 Oct 2000 12:12:05*

Speaking of altering photographs for public relations purposes, the University of Wisconsin isn't the only organization engaging in such dishonest activities. The Scientology organization did much the same thing at the beginning of the year -- only worse: They replicated people in photographs to try to deceive the media about the number of followers they have in their cult, not counting on the likelihood that anyone would notice.

For these photographs go to <http://www.lermanet.com/PhotoLIES.htm>  
One newspaper article about it: <http://www.lermanet.com/nohead.htm>  
Original CNN article: <http://www.cnn.com/2000/US/09/20/photo.fix.ap/index.html>

The risks here? Don't believe everything you see.

---

## ✶ Re: 50 million adults at risk for `net illiteracy'

"K Parker" <kparker@eudoramail.com>

*Thu, 12 Oct 2000 12:33:19 -0700*

> The report confirms the existence of a  
> "digital divide" that denies 65% of "lower  
> socioeconomic-status" Americans access to the  
> Internet, compared with only 17% in the top  
> income bracket.

This is too silly for words. Nobody is being "denied" anything by anyone here. Of course those of "lower socio-economic status" have more limited

resources than those at the top, but never has Internet access been more widespread or less expensive than today. And is the author actually asserting that 17% of those at the "top" are also being denied access?

---

## ✦ CFP: Risk Assessment & Policy Assoc. International Conference

"John M. Gleason" <jgleas@creighton.edu>  
*Mon, 9 Oct 2000 01:11:55 -0500 (CDT)*

The CFP for the 2001 Biennial International Conference of the Risk Assessment & Policy Association is posted at:

<http://cobweb.creighton.edu/gleason/rapa/cfp3.htm>

See the RAPA website for information about RAPA activities:

<http://www.fplc.edu/tfield/rapa.htm>

John M. Gleason, Vice President, RAPA, Dept of Information Systems & Technology  
College of Bus.Admin., Creighton University, Omaha, NE 68178 1-402-280-2624



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 21: Issue 10**

**Tuesday 7 November 2000**

## Contents

- [Pennsylvania county wins \\$1M for faulty computer voting machines](#)  
[David Banisar](#)
- [Thoughts on computers in voting](#)  
[Douglas W. Jones](#)
- [Security of electronic voting in public elections](#)  
[Avi Rubin](#)
- [Saturn made a bad assumption in my engine](#)  
[William Colburn](#)
- [I crashed because my phone was ringing](#)  
[Scott Gregory](#)
- [Unplanned roll in NASA's X-38](#)  
[James H. Paul](#)
- [\\*Lack\\* of barcode causes train to trap passengers](#)  
[Jeff Stieglitz](#)
- [No security in Internet-connectable laboratory instrument controller](#)  
[Stephen D. Holland](#)
- [Risk of using 'meaningful' file names](#)  
[Charles Bryant](#)
- [Re: Typo+"strange glitch"=private files world-readable](#)  
[Steve Summit](#)

● [REVIEW: "Virus Proof", Phil Schmauder](#)

[Rob Slade](#)

● [Info on RISKS \(comp.risks\)](#)

---

## ✂ **Pennsylvania county wins \$1M for faulty computer voting machines**

David Banisar <banisar@2rad.net>

*Thu, 2 Nov 2000 09:24:10 -0500*

A federal jury awarded Montgomery County, Penn., more than \$1 million Wednesday in a suit against an Indiana company that sold the county 900 computer voting machines that repeatedly broke down. The jury found MicroVote Corp. breached its implied warranties, but rejected all of the county's other claims, including fraud and breach of contract. The county had sought \$4.3 million against the company. [Source: \*The Legal Intelligencer\* <from <http://www.law.com>>]

---

## ✂ **Thoughts on computers in voting**

"Douglas W. Jones" <jones@cs.uiowa.edu>

*Tue, 7 Nov 00 16:43:41 CST*

It's election day, and as chair of the Iowa State Board of Examiners for Voting Machines and Electronic Voting Systems, it seems like a fair time to pause and think about the state of the art.

Over the past several years, an important trend has been evident in the

voting machines that have come before our board for approval in Iowa. This is the replacement of custom-built software with off-the shelf commodity software, usually some variant of Windows and largely dependent on Microsoft Office.

Computers in voting machines are old technology at this point, whether they're used for central count systems based on punched cards or mark sense readers, or whether they're precinct count systems based on mark sense or direct recording electronic voting machines. There are still lever machines in use, of course, but those haven't been changed in years and therefore, we don't see them coming up for examination.

Under the current Federal Election Commission guidelines for electronic voting systems, all custom-built software is subject to examination by an independent third party. On the other hand, "industry standard components" are acceptable, as is. The FEC has no enforcement power, but the FEC guidelines have been enacted into the voting law of numerous states.

The reason this concerns me is that we see a larger and larger fraction of the software inside the voting system becoming proprietary product of a third party and exempt from the requirement that it be available for a source code inspection. Furthermore, the size of commercial operating systems is immense, so an effective inspection is very hard to imagine!

What threat does this present?

If I wanted to fix an election, not this year, but 4 years from now, what I might do is quit my job at the University of Iowa and go to work for Microsoft, seeking to insinuate myself into the group that maintains the central elements of the window manager. It sounds like it might be fun, even if the job I'd need would largely involve maintenance of code that's been stable for years. My goal:

I want to modify the code that instantiates a "radio button widget" in a window on the screen. The specific function I want to add is: If the date is the first tuesday after the first monday in a year divisible by 4, and if the window contains text containing the string "straight party", and if the radio buttons contain, at least, the strings "democrat" and "republican", one time in 10, at random, switch the button label containing the substring "democrat" with any of the other labels, at random.

Of course, I would make every effort to obfuscate my code. Obfuscated coding is a highly developed art! Having done so, what I'd have accomplished is a version of windows that would swing 10 percent of the straight party votes from the Democratic party to the other other parties, selected at random. This would be very hard to detect in the election results, it would be unlikely to be detected during testing, and yet, it could swing many elections!

This is just one example attack! There may be similar vulnerabilities, for example, in the off-the-shelf database packages being used for

ballot  
storage and counting.

I don't mean to this example to reflect any ill feelings toward Microsoft,  
but it is true that their software is used in the vast majority of new  
voting systems I've seen. This threat does not require any cooperation from  
the vendor of the window manager or other third party component exempt from  
source code inspection. All it requires is a mole, working their way into  
the vendor and producing code which is not detected by the company's  
internal testing and inspection. Obfuscation is easy, and the art of the  
"easter egg" in commercial software makes it very clear that huge numbers of  
unofficial features are being routinely included in commercially released  
software without the cooperation of the software vendors. (OK, I know that  
some easter eggs are officially approved.)

Having said this, it is worth noting that Microsoft has indicated a  
preference about the outcome of today's presidential election, and there are  
excellent reasons to treat proprietary software produced by a partisan  
agency with great suspicion when it is included in a voting system!

My conclusion? The time has come for computer professionals to press for a  
change to the guidelines for voting machines, asking that all software  
included in such machines be either open source, available for public  
inspection, or at least open to inspection by a third party independent  
testing authority. There are no technical obstacles to this!

Linux, Free

BSD and several other fully functional operating systems are available and will run on the hardware currently being incorporated into modern voting machines!

But, this is not the end of the problem! How do you prove, after the fact, that the software in the voting machine is the software that was approved by the board of examiners and tested by the independent testing authority? No modern machine I'm aware of makes any real effort to allow this proof, although several vendors do promise to put a copy of their source code in the hands of an escrow agency in case a question arises.

Doug Jones <jones@cs.uiowa.edu> <http://www.cs.uiowa.edu/~jones/voting/>

[Note: Doug, Rebecca Mercuri <Mercuri@gradient.cis.upenn.edu> is just putting the finishing touches on her PhD thesis on the subject of electronic voting, at the University of Pennsylvania. I highly recommend you contact her for a copy, which should be available very soon. For everyone else, we will announce it here when the thesis is ready. Also, my book \*Computer-Related Risks\* has lots of background on risks in electronic elections and what to do about them. Rebecca has carried the analysis much further than I did. Her thesis will be a very valuable contribution that significantly raises the bar as to what should be demanded, not just hoped for, plus an analysis of the residual risks that would still remain. PGN]

## ✶ Security of electronic voting in public elections

Avi Rubin <rubin@research.att.com>

*Fri, 20 Oct 2000 15:46:02 GMT*

I recently participated in an interesting workshop sponsored by the NSF by request of President Clinton on the feasibility of e-voting in public elections. The workshop web page is <http://www.netvoting.org/>

From the Web site:

"On October 11 & 12, 2000, the Internet Policy Institute (IPI) will conduct a workshop to examine the issues associated with conducting public elections via computer networks. Sponsored by the National Science Foundation (NSF) and chaired by C.D. Mote, Jr., president of the University of Maryland, this workshop is part of a request by the White House to study the feasibility of Internet voting."

It was a collection of technical experts, Social Scientists, election officials, the Department of Justice, and the NSF. The workshop was fascinating. The technical participants were:

Erich Bloch, Washington Advisory Group

Lorrie Cranor, AT&T Labs - Research

Michael Fischer, Yale University

Dan Geer, @Stake, Inc.

Lance Hoffman, George Washington University

David Jefferson, Compaq Systems Research Center

Carl Landwehr, Mitretek Systems, Inc.  
Raymond Miller, University of Maryland  
Adam C. Powell, III, The Freedom Forum  
Ron Rivest, Massachusetts Institute of Technology  
Avi Rubin, AT&T Labs - Research  
Barbara Simons, Association for Computing Machinery

I spoke about security challenges/risks associated with remote electronic voting related to host security and Internet availability. I was asked to write up my comments. The paper is available at <http://avirubin.com/e-voting.security.html>

Avi Rubin <http://avirubin.com/>

[Added at PGN's request]

The workshop (<http://www.netvoting.org/>) held in October in DC was sponsored by the NSF by directive from President Clinton to study the feasibility of electronic voting in public elections. Subject matter experts were invited from the social science community, the technical and security community, election officials, and representatives from the department of justice. The meeting was chaired by Dan Mote, the president of the University of Maryland.

Panels were held discussing issues such what e-voting means, whether or not e-voting would improve accessibility, whether it would widen the digital divide, and whether more people would vote. On the technical side, there were panels about the security requirements, the current state of security on desktops as related to voting.

The mandate was to cover the following issues:

\* How to ensure the security and reliability of the voting process;

- \* How to protect the privacy of voters;
- \* How to authenticate voter identity;
- \* How to achieve broad and equitable access to online voting systems;
- \* How to assess the impact of online voting on representative democracy and community; and
- \* How to ensure that online voting systems are convenient, flexible, and cost-effective.

The group is going to produce a report that will be submitted to the White House and to Congress and to election officials all over the country.

My participation was as a panelist on security. I wrote up my comments.

They are available at <http://avirubin.com/e-voting.security.html>

Avi

---

## **✶ Saturn made a bad assumption in my engine**

"Schlake ( William Colburn )" <schlake@nmt.edu>

*Tue, 7 Nov 2000 13:33:56 -0700*

I have a 1-year-old Saturn. As a safety feature, my Saturn will prevent me from going faster than is safe with my suspension or tires. When I first got the car, I had to try this feature out, so I found a long straight road and floored it. When I got to 105MPH the engine lost power and I slowed down. Experimentation revealed that I couldn't regain power until I dropped below 100, then I could accelerate again.

A couple of days ago I drove through a fairly steep chasm with a road straight down one side and up the other. I figured I needed as much momentum as possible, so I pushed the clutch in and coasted down. Somewhere along the way I hit 105MPH. Just as I was starting up the opposite side I noticed that virtually all of my warning lights were on, and the engine was at 0RPM. A still engine means no power steering and no power brakes. I'm quite glad there weren't any turns or traffic that might have forced me to turn or brake.

The problem was the assumption that I got to an excessive speed by using the engine to accelerate. The default action works great when the clutch is engaged. In my case, I ended up with a car that suddenly became very hard to control when I was already doing something unsafe.

---

## **⚡ I crashed because my phone was ringing**

"Gregory, Scott" <Scott.Gregory@CIBC.CA>

*Mon, 23 Oct 2000 13:44:00 -0400*

On Yahoo news today, they carried this message from the Reuters feed

"Smart Tires to Warn Drivers Via Mobile Messages".

[http://dailynews.yahoo.com/h/nm/20001023/tc/tires\\_phones\\_dc\\_1.html](http://dailynews.yahoo.com/h/nm/20001023/tc/tires_phones_dc_1.html)

It details impending tire developments from Finland to put Bluetooth enabled

chips in their product. The tire will phone the driver if the pressure drops too low. Future developments include detection of wear, as well as hydro-planing (tire losing contact with the road due to water).

Standard security type risks, which phone gets the message?

Even better, timing and distraction risks. Like the fighter pilot with so much information that they cannot cope, the modern driver may soon have a phone ringing that they are losing control of the car.

"Really officer, it was an important call from my car that I had to answer.

And see, I did hit the tree it told me I was going to."

Reading my analog speedometer. sdg

---

## **✂️ Unplanned roll in NASA's X-38**

"James H. Paul" <jpaul@CapAccess.org>

*Mon, 6 Nov 1972 16:46:10 -0500 (EST)*

\*Aviation Week & Space Technology\*, 6 Nov 2000, p. 24

"NASA's X-38 Vehicle 131R did a slow, 360-deg. roll after release from its B-52 carrier aircraft on Nov. 2. It was the first free flight of the vehicle, which automatically stabilized under the preprogrammed deployment of a drogue chute and made a successful landing under parafoil on a dry lakebed runway, as scheduled, at Edwards AFB, Calif. The vehicle sustained no damage in the test. Project officials said they would have to do some

trouble-shooting to figure out why the Crew Return Vehicle (CRV) prototype rolled at an estimated average rate of about 20 deg. per sec. during its 24 sec. of scheduled free flight. A software problem in the vehicle's flight control system was suspected, although project officials were also looking at whether aerodynamic disturbances immediately after separation might have played a role. Actual separation from the B-52 was clean, and the flight control system maintained angle of attack throughout the 18-sec. roll. The vehicle is an 80%-scale version of the CRV designed to provide emergency escape for International Space Station crews."

There's an F-16 test pilot somewhere thinking, "Been there, done that."

James Paul Annandale Virginia <jpaul@capaccess.org>

---

## **\*Lack\* of barcode causes train to trap passengers**

<Jeff\_Stieglitz@toyota.com>

*Fri, 20 Oct 2000 15:09:22 -0700*

Dozens of travelers were stuck on an underground passenger train at Denver

International Airport on 19 Oct 2000 after a computer problem sent the

train shooting past the main terminal. It took workers about 20 minutes

to move the train to a station, where passengers got off. No one was

injured. A circuit board on the automated train lost its memory and

failed to read a bar code that signals it to stop. The train overshot the station and safety mechanisms kicked in. [Source: AP item, 20 Oct 2000, PGN-ed]  
<http://www.cnn.com/2000/WORLD/europe/france/10/20/france.trial/index.html>

The RISKS archives are full of engineering designs without fail-safe features. One would think that the train would have a hardware interlock to stop it if something disturbed the computer. Fail-safe also suggests that sensor events are required to enable and maintain motion rather than stop it. The lack of sensor input or keep-alive should result in a graceful shutdown.

I'd guess that this train requires a computer to unlock the doors, rather than a fail-safe design that would require the computer to keep them locked.

---

## **⚡ No security in Internet-connectable laboratory instrument controller**

"Stephen D. Holland" <sdh4@tam.cornell.edu>  
*Fri, 20 Oct 2000 15:36:25 -0400*

National Instruments (<http://www.ni.com>) sells a device for gatewaying between ethernet (TCP/IP) and the IEEE-488 (GPIB) bus commonly used for controlling laboratory instruments, such as oscilloscopes, voltmeters, motion-controllers, etc.

I was somewhat astounded, upon purchase of this device, to find that it had no security whatsoever. That is, if you properly configure it and attach it to your instruments, anyone in the world with the proper software can control your lab equipment. Worse, there is no mention in any of the documentation or marketing materials that security is an issue.

The manual even suggests "If you are directly linked to the Internet... you can contact the... support department to update your firmware." without any consideration of the risks of the device being connected. Marketing materials also promote Internet-connected use without discussion of the risks involved.

Securing this device requires putting it on its own ungatewaged ethernet segment. This is not mentioned in the manual, and reduces the utility of the device (cannot share existing wiring).

The RISKS:

- End users could unknowingly assemble systems that are open to attack or accidental disruption by intruders. Most laboratory scientists are not particularly well-versed in the minutiae of network security. As GPIB is commonly used for mechanical control, there is the real danger of physical damage.

- Security issues are still sufficiently esoteric that a respected and generally competent company such as National Instruments can develop (and market for several years) a device for the

Internet that has no security whatsoever.

I am hoping that National Instruments can develop a firmware update that adds at least a minimal passcode for access control.

Steve Holland, Dept. of Theoretical and Applied Mechanics,  
Cornell University  
sdh4@tam.cornell.edu

---

## **⚡ risk of using 'meaningful' file names**

Charles Bryant <ch@chch.demon.co.uk>

*5 Nov 2000 23:36:26 -0000*

A Milton Keynes Council worker sent a reply to one or more people who were commenting on proposals for a travelers' halting site. The letter had an embarrassing addition to the intended text. In small letters at the bottom was the file name: "H:\Gypsy letter to whingers.doc".

Of course this risk is equally the risk of not proof-reading a printed copy.

Charles Bryant - ch@chch.demon.co.uk

---

## **⚡ Re: Typo+"strange glitch"=private files world-readable ([RISKS 21.09](#))**

Steve Summit <scs@eskimo.com>

*Sat, 4 Nov 2000 06:30:37 -0800 (PST)*

I'm not sure why "no one was sure exactly what triggered the glitch". It's reasonably obvious what happened: a sensitive file was accidentally left in a directory the web server could get to, the local search engine dutifully indexed it, and from then on it was sitting there just waiting for someone's search to unearth it.

Steve Summit <scs@eskimo.com>

---

## ⚡ REVIEW: "Virus Proof", Phil Schmauder

"Rob Slade, doting grandpa of Ryan and Trevor" <rslade@sprint.ca>

*Mon, 23 Oct 2000 08:18:27 -0800*

BKVRSPRF.RVW 20000711

"Virus Proof", Phil Schmauder, 2000, 0-7615-2747-8,  
U\$34.99/C\$48.95/UK#32.49

%A Phil Schmauder

%C 3875 Atherton Road, Rocklin, CA 95765-3716

%D 2000

%G 0-7615-2747-8

%I Prima Publishing/Jamsa Press

%O U\$34.99/C\$48.95/UK#32.49 800-632-8676 www.primapublishing.com

%P 273 p. + CD-ROM

%T "Virus Proof: The Ultimate Guide to Protecting Your PC"

On the very first page of this book we are told that viruses are written to steal or destroy "information that resides on your disk." (Viruses are written to reproduce.) The text then contradicts itself by saying that viruses may just print a message. Then we are told that you

should never  
run programs downloaded from the Internet (downloading infected  
program  
files has always been a relatively trivial vector). Along the  
way we are  
told such vital information as that viruses must get into your  
computer's  
RAM in order to do damage (\*everything\* has to get into your  
computer's RAM  
in order to do anything) and that viruses are exchanged on disks  
or  
transferred files (that pretty much covers the field of data  
transport,  
wouldn't you say?)

Welcome to "Virus Proof," a collection of mistaken, valid,  
useless, and  
repetitive information. Sharp-eyed readers will have noted the  
inclusion of  
"valid" in that list. Unfortunately, you will have to be much  
more acute to  
pick out the true facts from the volume under discussion. As  
the old saying  
goes, if you can tell good advice from bad advice, you don't  
need any  
advice.

Some of the errors in the book simply show that the author has  
not done his  
homework. (There is no evidence to suggest that the  
Michelangelo virus was  
written to "commemorate" the birth of Michelangelo the artist.  
The  
researcher who first reported the existence of the virus learned  
that the  
target date of March 6 was Michelangelo's birthday, and so used  
that name as  
a convenient label.) Some of the errors in the book are more  
seriously  
misleading. (The Michelangelo virus did not "occur" on March 6,  
1992. It  
was, fortunately, discovered long before, possibly existed  
before March of

1991, and still results in regular computer erasures every March 6th to this date.)

The author does keep telling the reader not to use any data file, or run any program, until it has been scanned for viruses. That is good advice, as far as it goes. Unfortunately, it isn't very useful advice, and the constant repetition of that single injunction is likely going to dull the reader to the necessary finer points.

The directive to scan everything isn't the only thing that gets repeated in the book. The first chapter manages to tell us once per page that computer programs are lists of instructions. Now, that statement is true: programs are sets of commands. But that bald assertion provides the normal computer user with no insight that could help with virus protection. One would think that the space dedicated to this piece of trivia could more helpfully be employed in presenting an accurate definition of viruses, or a list of the ways that you are more likely to get a virus these days.

In only four pages, chapter two presents serious misinformation. A boot sector does not show up on a list of files on a disk. Boot sector infectors can infect non-bootable, and even "blank" disks. Trojan horse (or just "trojan") programs do not reproduce. A file infecting virus is not referred to as a "Trojan Horse virus." The definition given for a worm (if you are making a distinction the term "worm virus" makes no sense) clearly contradicts the declaration that a worm could also be a file

infector. Most macro languages are not capable of supporting a successful virus: to date, only those written for Microsoft applications have presented any danger.

And so it goes. Virus writers don't need your password, and system security breakers (who dearly love the confusion of the term "hacker") don't bother with viruses. Being the first on your block to upgrade to new versions of programs can have drastic security risks itself. If you are not supposed to run anything you download from the Web, why are you supposed to upgrade your software over the Internet? Since viruses are appearing at the rate of hundreds per month, keeping up with the few that make it into [large AV corporation]'s press releases is unlikely to be very useful. Mailing lists and newsgroups are recommended without any analysis. Most recent email viruses and worms harvest addresses for regular correspondents, so the direction to avoid email attachments from someone you don't know is almost worthless. Firewalls have nothing to do with viruses. If a virus infects a system file, knowing what programs are running on your computer is useless. Many loopholes have been found in the security of ActiveX controls: restricting operation to signed controls provides very little protection. Backups will help you recover if hit, but provide no inherent virus protection. Knowing how to break into systems will not protect you from viruses, nor will seven pages of C source code for a variant of the Crack program. (For those script kiddies eager to learn how to break

into  
systems, save your money. It doesn't tell you that, either.)  
Phone  
phreaking isn't that easy, trying the stuff in the book can get  
you  
arrested, and it has nothing to do with viruses. (And John  
Draper's own  
account, given on the site illustrated, contradicts the story in  
the book.)  
Chernobyl is a variant of CIH, and not the other way around.  
Backing up the  
Registry provides no inherent virus protection. Anonymizers for  
email and  
Web browsing have nothing to do with viruses. Cookies have  
nothing to do  
with viruses. (Many of the points made about cookies are  
incorrect as  
well.) Happy99 used Usenet news, as well as email. Spam has  
almost nothing  
to do with viruses (and most of the recommended actions are not  
only  
useless, but will annoy people who have better things to do).  
The material  
on virus hoaxes is limited, physically hard to read (small  
print), and has  
no real analysis. Chat has nothing to do with viruses. Denial  
of service  
attacks have little to do with viruses, chapter sixteen has  
\*nothing\* to do  
with viruses, and neither do six pages of SYNattack source  
code. Privacy  
has nothing to do with viruses (and chapter seventeen has little  
to do with  
privacy). Email encryption has nothing to do with viruses. The  
Melissa  
virus was not polymorphic. Polymorphic viruses do not change  
their  
payloads. Virus "families" result from virus writers taking a  
given virus  
and making very minor changes to it. Digital signatures have  
little to do  
with viruses, and chapter nineteen does not discuss key  
management at all.

JavaScript is not a "cut down" version of Java, and does not have Java's security model. E-commerce does not have anything to do with viruses. Y2K does not have anything to do with viruses. And, fortunately, the code presented in chapter twenty five is nowhere near sufficient to create a working virus. (It is enough to create serious problems for the person who tries to use it.)

Now, of course, a number of the items mentioned do have something to do with general security. Unfortunately, the level of detail given in the book is far from sufficient to protect the user against these threats. Indeed, the threats themselves are not described particularly well, and I could go through a very similar exercise in pointing out the weaknesses in the general security material.

Given the total size of the book it really isn't a work on viruses. It throws together a random assortment of information (and misinformation) about a variety of security related topics. Nothing is covered in depth, and nothing is covered completely accurately. Approximately half of the book is occupied with screenshots of miscellaneous Web sites, not always to do with the topic under discussion (and a number of which are repeated at random through the work) so this detracts even more from the material that could have been provided.

A pamphlet on viruses surrounded by some opining on security issues buried within a lot of careless research.

copyright Robert M. Slade, 2000 BKVRSPRF.RVW 20000711  
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 21: Issue 11**

**Weds 8 November 2000**

## Contents

- [Did a human factors problem affect the U.S. presidential election?](#)  
[Steve Bellovin](#)
- [More on Florida in this and previous elections](#)  
[PGN](#)
- [E-voting as a panacea for Florida count?](#)  
[Jeremy Epstein](#)
- [CNN: E-voting could have prevented U.S. election chaos](#)  
[Evan McLain](#)
- ["REALITY RESET": "Hacking the Vote"](#)  
[Lauren Weinstein](#)
- [Web sites report exit poll results before networks do](#)  
[NewsScan](#)
- [Political dirty tricks, cyber-style](#)  
[NewsScan](#)
- [Vote auction Web site moves operations overseas](#)  
[NewsScan](#)
- [UK air-traffic control problems](#)  
[PGN](#)
- [Indianapolis FAA route center running on generators for a week](#)  
[Nathan Brindle](#)

- [Raccoon power outage over the weekend](#)  
[Dan Ellis](#)
  - [Researchers able to defeat digital music security measures](#)  
[NewsScan](#)
  - [Verisign and MS authenticode](#)  
[Carl Byington](#)
  - [Microsoft Web site vandalized](#)  
[NewsScan](#)
  - [The latest in anti-spam technology](#)  
[Greg Compestine](#)
  - [Re: EMI, etc.](#)  
[Pete Mellor](#)
  - [2001 USENIX Annual Technical Conference - Call For Papers](#)  
[Andrea Galleni](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

## ✶ **Did a human factors problem affect the U.S. presidential election?**

Steve Bellovin <smb@research.att.com>

*Wed, 08 Nov 2000 14:15:47 -0500*

The outcome of the U.S. Presidential election may have been determined by poor human factors in a computerized vote-casting system.

As of this writing (early afternoon on Wednesday), Bush and Gore are separated by less than 1800 votes (.03%) in Florida. Due to the arcana of U.S. election law, whoever carries Florida at this point will win the overall election. And there's a problem in one county that may have resulted in ~3000 votes that were intended for Gore in fact being cast for Buchanan, a minor party candidate.

Palm Beach County uses a punch-card voting system. Because of the layout of the names relative to the holes and the buttons to punch those holes, it was apparently easy to get confused about how to vote for Gore. Apart from all the calls to the election board by confused voters, there is circumstantial evidence from the actual tally: Buchanan drew 3407 votes in this county, more than anywhere else in the state, and considerably at variance with both the usual demographics (this county is heavily Democratic, and would be expected to vote for Gore) and with the number of votes Buchanan received in similar, neighboring, larger counties (789 in Broward; 561 in Miami-Dade County).

The director of the state Department of Elections doesn't think there's a problem -- but he was appointed by Jeb Bush, governor of Florida and brother of the Republican presidential candidate...

--Steve Bellovin

---

## **✶ More on Florida in this and previous elections**

"Peter G. Neumann" <Neumann@CSL.sri.com>

*Wed, 08 Nov 2000 16:17:09 PST*

In addition to the Palm Beach County curiosity noted by Steve Bellovin, a heavily loaded ballot lock box was found today in a heavily Democratic

precinct. I don't think this is what Al Gore meant by a "Lock Box on (Social) Security."

[CORRECTION ADDED IN ARCHIVE COPY: Apparently this box contained

supplies, not ballots. But \*The NY Times\* 10 Nov noted various precincts in which ballot boxes and a bag of cards had not been included in the original count.]

For some historical perspective, we might recall the 1988 election in Florida, in which there were 200,000 fewer votes for the Senate race than for the presidential candidates, and the remarkable anomaly was mostly only in four counties administered by a particular computer system vendor. The declared winner was Connie Mack, who has just retired, 12 years later. See \*The New York Times\*, 12 Nov 1988, and [RISKS-7.78](#).

And then there was the St Petersburg city election in March 1993 in which 1429 votes were recorded for the incumbent mayor tabulated under an industrial precinct that had ZERO voters, where the mayor won the election by 1425 votes. Fuzzy math strikes again? See Rebecca Mercuri, Corrupted Polling, Inside Risks, \*Communications of the ACM\*, vol 36 no 11, Nov 1993, p.122, on her Web site at <http://www.seas.upenn.edu/~mercuri/mynewhome/Papers/corripoll.html>

I would not trust a computerized voting system even if I had written it myself, because of the many ways in which such systems can be subverted.

(Last night's events will undoubtedly slow down the final wrapup of Rebecca's PhD thesis noted in [RISKS-21.10](#), because there is more

potential  
grist for her mill -- not just in Florida, but in other states  
as well.)  
PGN]

---

## ✶ E-voting as a panacea for Florida count?

"Jeremy Epstein" <jepstein@webmethods.com>  
Wed, 8 Nov 2000 15:28:02 -0500

<http://www.cnn.com/2000/TECH/computing/11/08/e.voting.no.gamble.idg/index.html>

An article on CNN.com quotes "experts" as saying that the problems getting an accurate vote could have been avoided if everyone used electronic vote counting technology. [Note: not online voting... just electronic voting machines.]

The article says in part "'Of course you would have 100 percent accuracy with electronic voting. That would prevent the necessity of a recount,' said Hans van Wijk, who markets electronic voting systems for Groenlo, Netherlands-based Nedap. In the Netherlands, some 80 percent of precincts use e-voting, he said."

As has been discussed numerous times in RISKS (including yesterday in [RISKS-21.10](#)), electronic counting is certainly not 100% accurate. But if this is what the public thinks of electronic counting, will there be the same naive expectations about accuracy of online voting? The article talks about that too (quoting someone from Baltimore Technologies as

saying

"Online voting would not only dramatically reduce the count time but also ensure a more reliable initial result"). There is an acknowledgement that online voting has its own dangers, noting the risks of accurate identification of users, denial of service, and malicious attacks. No recognition though of the risks of just plain malfunctioning software, though.

Gotta go. All this gore-y discussion of a recount in Florida has me bush-ed.

--Jeremy

[For those of you who have not seen it, PLEASE read the People For Internet Responsibility Statement on Internet Voting:

<http://www.pfir.org/statements/voting>

PGN]

---

## **⚡ CNN: E-voting could have prevented U.S. election chaos**

McLain Evan M CPT <mclaine@lewis.army.mil>

*Wed, 8 Nov 2000 19:43:29 -0000*

CNN's story about voting technology, on-line and otherwise:

<http://www.cnn.com/2000/TECH/computing/11/08/e.voting.no.gamble.idg/index.html>

An interesting quote from the article: "But Dublin-based electronic security company Baltimore Technologies said reliability is no problem. "Online

voting would not only dramatically reduce the count time but also ensure a more reliable initial result," said a spokeswoman. She added that online voting would help older, ill, and disabled voters to take part in the polls."

RISKS readers will be happy to see there is also a discussion of potential fraud and security risks.

Evan McLain <evan.mclain@bigfoot.com>

---

## ⚡ "REALITY RESET": "Hacking the Vote"

"Reality Reset" <reality@vortex.com>  
*Wed, 8 Nov 2000 12:46:51 -0800 (PST)*

"REALITY RESET"

<http://www.vortex.com/reality>

by

Lauren Weinstein (lauren@vortex.com)

November 8, 2000

Today's Edition:

"Hacking the Vote"

<http://www.vortex.com/reality/2000-11-08>

To subscribe or unsubscribe to/from this list, please send the command "subscribe" or "unsubscribe" respectively (without the quotes) in the body of an e-mail to "reality-request@vortex.com".

"Hacking the Vote" (November 8, 2000)

"If they'd been listening to me all along, all of this election confusion could have been avoided," said Paddy Mastoid.

Paddy is the president of trust-us-not-to-badly-screw-up-your-vote.com, a firm promoting Internet voting systems. I found 12 messages from him on my voicemail this morning, as the nation awoke to the bizarre aftermath of election day, with a historically close election still undecided and the U.S. population swinging slowly in the wind.

"Look at this mess," said Paddy. "Now they have to re-count all those votes in Florida, there are concerns over voting irregularities down there, and we might well end up with a President who didn't even win the popular vote! Talk about not having a mandate. And I could have prevented all of this hassle!"

"How so?" I asked.

"Basically, our plan is to eliminate all those long lines at those obsolete polling places. We want to toss the antiquated paper ballots, punch cards, and mechanical voting machines out the window. We'll let people vote online using the same home and office PCs that they already use for accessing offshore gambling sites and downloading porn."

"Hmmm. Sounds like a tempting goal, but aren't you worried about security, reliability, all that sort of stuff?" I asked.

"Hey, we didn't just fall off the turnip truck. We're using secure,

redundant Web servers, so your vote will be just as safe as your credit card numbers during online purchases," said Paddy. "You're happy buying things online, aren't you?"

"Well, no, not really, not with all of the security breaches at sites that were supposed to be secure, and their compromising of personal information. I realize that things can go wrong with old-style voting systems, especially if they're set up badly, but at least with them it's usually possible to do various forms of meaningful re-counting when there's a question about an election's validity."

"But that's my whole point!" said Paddy. "Look at all the trouble being caused by even being \*able\* to do a physical re-count. Wouldn't it be better to have a nice, computerized system where all the votes are electronic and stored safely in computers where nobody but programmers, system administrators, and top election officials can screw around with them? You don't think any of those guys would mess things up do you? When it's all in the computer, you don't have any \*choice\* but to trust the computer! You can't really re-count so there'd be no point to complaining. Problem solved!"

"Hmmm. What about hackers? If these systems are on the Internet, they'd seem just as vulnerable to attack and manipulation as any other so-called secure sites."

"Not to worry!" said Paddy. "We ran a contest and invited hackers to crack

our demonstration system. Five people tried and the only guy who got in was a 12 year old kid in West Palm Beach, and he promised cross-his-heart not to tell anyone how after we gave him a DVD player! No problem there."

"But why would most hackers even want to tip their hands by playing with your demo sites? Wouldn't the real pros just wait until a real election and then flood your servers with garbage to block real voters out? Couldn't they plant surprises in unrelated downloads that could hide on people's PCs for months or years before being activated on election day to disrupt or manipulate the voting process? There's really no way to secure the typical operating systems that most people have on their home or office computers from those sorts of attacks," I said.

"Picky, picky, picky!" said Paddy. "I say let's just deploy these Internet voting systems now and keep the people happy. If these hypothetical hackers you're talking about are really that good, we probably wouldn't even realize that they'd been screwing around with the election anyway. Ignorance can be bliss. And that would sure be preferable to all the hassles they're having in Florida today!"

"I really don't think that's necessarily true ..."

"And at least we wouldn't have network TV anchors getting punchy from being up all night!" said Paddy.

"You do have a point about that," I said.

"I knew that I could convince you, Lauren."

--Lauren--

Lauren Weinstein,  
lauren@pfir.org or lauren@vortex.com or lauren@privacyforum.org  
Co-Founder, PFIR - People For Internet Responsibility - <http://www.pfir.org>

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

Member, ACM Committee on Computers and Public Policy

Copyright 2000 by Vortex Technology. All rights reserved.

This item may be freely redistributed so long as it is complete and includes this notice.

---

## Web sites report exit poll results before networks do

"NewsScan" <newsscan@newsscan.com>

*Wed, 08 Nov 2000 09:12:36 -0700*

Whereas mainstream news organizations were bound by self-imposed rules

preventing them from releasing state exit poll results before the polls

closed, a number of politically oriented Web sites leaked the results as

soon as they were available. Voter News Service (VNS), the consortium of

news organizations that conducted the exit polls, is threatening to bring

legal action against the sites that leaked early results, including

DrudgeReport.com and Inside.com -- which, however, indicated that they

obtained the information not from VNS but from unidentified sources.

Inside.com editor Michael Hirschorn said that he had received e-mail leaks

from dozens of mainstream journalists, and that the public have as much

right to know that kind of information as journalists do. He added: "The genie is out of the bottle, and it's wishful thinking that you could put it back in. Once this information is out, thanks to e-mail and the Internet, it becomes incredibly easy to distribute." [AP/\*San Jose Mercury News\*, 7 Nov 2000 <http://www.mercurycenter.com/svtech/news/breaking/ap/docs/6063841.htm>; NewsScan Daily, 8 Nov 2000]

---

## **⚡ Political dirty tricks, cyber-style**

"NewsScan" <[newsscan@newsscan.com](mailto:newsscan@newsscan.com)>  
*Wed, 08 Nov 2000 09:12:36 -0700*

In the closing hours of the election campaign the site of the Republican National Committee (RNC) was vandalized by hackers who urged visitors to vote for Gore. The Democratic National Committee (DNC) denied it had any connection to the act of vandalism, and said intruders had forced the shut-down of the DNC's external e-mail system. [AP/\*USA Today\*, 7 Nov 2000 <http://www.usatoday.com/life/cyber/tech/cti782.htm>; NewsScan Daily, 8 Nov 2000]

---

## **⚡ Vote auction Web site moves operations overseas**

"NewsScan" <[newsscan@newsscan.com](mailto:newsscan@newsscan.com)>  
*Thu, 26 Oct 2000 09:44:02 -0700*

A Web site offering to sell 21,000 votes for President to the highest bidder has changed its domain name and transferred its registration to a company based in Germany. The [www.vote-auction.com](http://www.vote-auction.com) site asks visitors to fill out personal details and then offers to sell the votes in blocks broken down by state. The goal, according to the Web site, is to bring "the big money of campaigns directly to the voting public," but the owners, who are Austrian, say they still need to work out the details of how everyone would get paid, and how to verify that they cast the right ballot. The site has been criticized by election officials in Michigan, New York and other states, but as of its reopening this week, more than 2,500 California voters had offered their votes and the leading bid was \$48,000, or \$19.61 per vote. In August, six people offering to sell their votes for President drew bids as high as \$10,000 on eBay before the online auctioneer shut them down. [AP 25 Oct 2000 <http://news.excite.com/news/ap/001025/20/votes-for-sale>; NewsScan Daily, 26 Oct 2000]

---

## **✶ UK air-traffic control problems**

"Peter G. Neumann" <Neumann@CSL.sri.com>  
*Sat, 04 Nov 2000 20:27:12*

If you are interested in aviation safety, you might want to

check out

<http://www.pprune.org>, click on "Forums", and then "rumors and news", for a remarkable collection of computer problems related to ATC in the UK.

---

## **Indianapolis FAA route center running on generators for a week**

Nathan Brindle <nbrindle@netdirect.net>

*Tue, 07 Nov 2000 23:45:58 -0500*

A week later, the FAA route center at Indianapolis is still running on backup generator power ever since a 31 Oct 2000 power outage that "caused flight delays and at least two close encounters between airplanes". The cause of the original outage was still unknown. The route center has 6 diesel generators, three of which are used normally and the other three are for backup. However, after the outage, the diesels fired up, but the main radar could not be brought back up. The 70 controllers had to had planes off to other centers. Close calls were reported by a private jet and a USAir flight. Onboard collision avoidance was given credit for avoiding any tragedies. [Source: An article in the \*Indianapolis Star\*, 7 Nov 2000 (Generators used for flight routing as a precaution, by Terry Horne); PGN-ed]

---

## **⚡ Raccoon power outage over the weekend**

Dan Ellis <ellisd@cs.ucsb.edu>

*Mon, 6 Nov 2000 11:19:42 -0800 (PST)*

I received the following e-mail on a Monday afternoon (after the problems had been fixed). Several physical devices had been damaged (network hubs and switches) at UC Santa Barbara making for a very unproductive time for many employees and students and for a very stressful time for facility and system administrators.

The point: the weak link will be found and exploited by somebody or something, causing discomfort to us all. Malicious intent is not a prerequisite.

Dan Ellis, PhD student, UCSB, ellisd@cs.ucsb.edu (805) 893-4394

> Date: Mon, 06 Nov 2000 08:33:55 -0800

> From: dragon@ece.ucsb.edu

> To: coe-notify@engineering.ucsb.edu, all-grad@engineering.ucsb.edu

> Subject: power outage over the weekend

> Information only --

> A bit after midnight Friday/Saturday, a raccoon strolled into the power

> substation that serves this end of campus and got across a transformer

> that takes the 16kV line down to 4160VAC. The raccoon paid the price for

> this, and he is now merely a warning example of how fragile our power

> infrastructure can be.

> However, various buildings on campus also paid a price, as all

power on

> the "A" feeder was off line for nearly two hours.

> Some functions in some buildings had not been restored by this morning,

> however, including HVAC and equipment chilled water in Engineering 1.

> Almost all this equipment is now back in operation. You may wish to check

> computers and process controllers to determine if harm was done during

> this outage.

[A Rocky Raccoon gets added to the long list of Reubened Mammalians.

Must have been Raccoonoitering. After all, it was noit toim, even

if not Down Under! PGN]

---

## **🔥 Researchers able to defeat digital music security measures**

"NewsScan" <newsscan@newsscan.com>

*Tue, 24 Oct 2000 08:17:09 -0700*

A team of computer scientists at Princeton and Rice Universities and the

Xerox Palo Alto Research Center (PARC) has been able to remove the invisible

"watermarks" used by the 200-company Secure Digital Media Initiative (SDMI)

to protect digital music files from pirates. SDMI had offered a prize

[[RISKS-21.05](#)] to anyone who could defeat its various security measures, four

out six of which make use of watermarks. SDMI's Tala Shamon said, "I

expected some would have fallen. This is part of an empirical process to get

the best technology." [AP/MSNBC 24 Oct 2000;  
<http://www.msnbc.com/news/480521.asp> NewsScan Daily, 24 Oct 2000]

---

## **⚡ Verisign and MS authenticode**

Carl Byington <carl@five-ten-sg.com>  
*Mon, 23 Oct 2000 13:04:59 -0700*

MS has an authenticode mechanism that allows publishers to digitally sign their code using certificates from Verisign. The code is signed via a MS program (signcode) with  
"-t <http://timestamp.verisign.com/scripts/timestamp.dll>";  
as an option.

The Verisign stuff is suppose to properly timestamp the signature, but their clock is very wrong!! I did the signature at 12:42, and the .exe now has a new modification timestamp of 12:42, but the certificate claims it was signed at 12:46. So we cannot really believe the times in any of these Verisign certificates.

<http://www.five-ten-sg.com>

---

## **⚡ Microsoft Web site vandalized**

"NewsScan" <newsscan@newsscan.com>  
*Fri, 27 Oct 2000 09:00:30 -0700*

Microsoft's internal computer network was invaded by "trojan

horse" software

that caused company passwords to be sent to an e-mail address in St. Petersburg, Russia. Calling the act "a deplorable act of industrial

espionage," Microsoft would not say whether or not the hackers may have

gotten hold of any Microsoft source code. [AP/\*The New York Times\*, 27 Oct

2000 <http://partners.nytimes.com/2000/10/27/technology/27WIRE-MSHACK.html>;

NewsScan Daily, 27 October 2000]

[The following issue of NewsScan on 31 Oct 2000 (Hallowe'en!) noted

Microsoft says the attack lasted only 12 days instead of the 5 weeks

reported earlier, and no major corporate secrets were stolen. PGN]

---

## ⚡ The latest in anti-spam technology

"Greg C" <gmc333@my-deja.com>

*Mon, 6 Nov 2000 08:27:47 -0800*

This morning I received a spam item that originated in a yahoo account. Yahoo seems to be pretty good at responding to spam, so I forwarded

a report to them. I noticed in the body of the email that there was the quasi-traditional "to unsubscribe send your email address" to an account at myrealmailbox.

So I did the obvious and forwarded the spam again to myrealmailbox (after first browsing their Web site trying in vain to find a policy towards spam.)

In return I received this reply:

>From: abuse@myrealbox.com  
>To: gmc333@my-deja.com  
>Subject: Automatic reply  
>Date: Mon, 06 Nov 2000 09:09:05 +119303947 (MDT)  
>  
>Novell and myrealbox.com are not responsible for this  
>mailing, it has not used our network or e-mail system. Novell  
>Internet Message System (NIMS) employs some of the most  
>sophisticated anti-spamming technology in the industry.  
>The sender fraudulently used myrealbox.com  
>IDs for replies or opt-out mails. These accounts  
>never existed or have been terminated. We are committed  
>to helping to eliminate this type of mail system  
>abuse.

The RISKS? Apparently the technology is so advanced it's learned the art of plausible deniability. There is also the RISK that a human will never find out what I originally complained about and modify the system appropriately.

Greg Compestine <http://homestead.deja.com/user.gmc333/index.html>

---

## ⚡ Re: EMI, etc. (Ladkin, [RISKS-21.08](#))

Pete Mellor <pm@csr.city.ac.uk>  
*Mon, 16 Oct 2000 22:46:01 +0100 (BST)*

Regarding the enormous convoluted problem of how much EMI is required to cause a spark and hence an explosion in a fuel tank (Re: EMI, TWA 800 and Swissair 111, from Peter B. Ladkin, [RISKS-21.08](#)), Andy Weir, in his book "The Tombstone Imperative" made a very simple suggestion:

Fill the vacant space above the fuel in the tanks with nitrogen,  
and any spark, however caused, cannot lead to an explosion.

Should not engineers welcome the most simple solution to a problem?

Should we not listen to people who are not engineers?

Peter Mellor, Centre for Software Reliability, City University,  
London EC1V 0HB  
+44 (0)20 7477 8422 Pete Mellor <p.mellor@csr.city.ac.uk>

---

## **2001 USENIX Annual Technical Conference - Call For Papers**

Andrea Galleni <andrea+nospam@usenix.org>

*Thu, 26 Oct 2000 17:28:02 -0700*

2001 USENIX Annual Technical Conference Announcement and Call  
for Papers

25-30 Jun 2001, Marriott Copley Place Hotel Boston,  
Massachusetts USA

<http://www.usenix.org/events/usenix01>

Sponsored by USENIX, the Advanced Computing Systems Association

FREENIX Refereed Track: November 27, 2000 General Session  
Refereed

Track: December 1, 2000 Notification to authors: January 31, 2001  
Camera-ready papers due: May 1, 2001. Program Chair: Yoonho  
Park, IBM Research

USENIX Conference Office

2560 9th Street, Suite 215

Berkeley, CA 94710

USA Phone 510-528-8649;

Fax 510-548-5738 email: [conference@usenix.org](mailto:conference@usenix.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 21: Issue 12**

**Saturday 11 November 2000**

## Contents

- [Sanity in the Election Process](#)  
[Lauren Weinstein and Peter Neumann](#)
- [Statement by Don A. Dillman on Palm Beach County Florida Ballot](#)  
[Rob Kling](#)
- [Florida vote counts](#)  
[PGN](#)
- [The end of the Multics era](#)  
[PGN](#)
- [Excessive bounce activity and lost messages](#)  
[PGN](#)
- [Info on RISKS \(comp.risks\)](#)

---

## ✶ Sanity in the Election Process

Lauren Weinstein <[lauren@vortex.com](mailto:lauren@vortex.com)>  
*Sat, 11 Nov 2000 13:29:47 -0800 (PST)*

Lauren Weinstein

Responsibility

Co-Founder, PFIR - People For Internet

Moderator, PRIVACY Forum

Member, ACM Committee on Computers and

Public Policy

Peter G. Neumann

Co-Founder, PFIR - People For Internet

Responsibility

Moderator, RISKS Forum

Chairman, ACM Committee on Computers and

Public Policy

FOR IMMEDIATE RELEASE

"Sanity in the Election Process"

November 11, 2000

The continuing controversies over the results of the recent U.S. Presidential election, particularly concerning the vote in Florida, have now apparently begun to hinge on technical issues relating to voting systems and ballots, especially in terms of machine vs. manual recounts, voting irregularities, voter confusion and complaints, and other related issues.

We feel that several critical points are being misunderstood or misrepresented by some parties to these controversies, particularly in light of Governor George W. Bush's campaign having taken federal court actions attempting to block manual recounts of the vote in several Florida counties. Regardless of the outcome of those particular court actions, the following points are crucial to consider.

1) As is well known to election officials and voting system vendors, but

historically not advertised to the public at large, all voting systems are subject to some degree of error -- electronic and mechanical systems alike. Punchcard-based systems are no exception, for which a variety of known problems can occur. These include poor ballot layout (currently a major issue regarding the "butterfly" Palm Beach County ballot), machine reading errors (often relating to incompletely punched ballot selections, usually in the form of "hanging chad"), paper fatigue, and other problems.

In general, so long as the interested parties both have observers participating in manual recounts to assure a consensus on the interpretation and tabulation of the cards, manual recounts provide the MOST reliable mechanism for counting these cards accurately, particularly due to the common hanging chad problem which often reads as "closed" (no vote) when processed through automatic reading machines. Indeed, manual counting is still prevalent today in England and Germany.

It is true that manual recounts tend to boost the number of votes counted, again due to hanging chad and other problems noted above. This suggests that if concerns are present regarding the fairness of a manual recount only in particular counties, the obvious solution is to manually recount in ALL Florida counties, and to manually count ALL votes (not just a sampling). Yes, this will be slow, and potentially expensive.

But if the will of voters is not to be subjugated to technical flaws over which they have no control, this would be the only fair

course.

2) While all voting systems have "normal" error rates, these errors typically

are not of great significance so long as the margin of victory is

significantly larger than the error rate, which is usually the case.

However, this does NOT suggest that systemic errors in the voting process

are of insignificance and can simply be discarded in close elections

where the error rate DOES matter.

In particular, the Palm Beach situation from the VERY START of election

day showed all the earmarks of systemic problems. Voters complained of

ballot confusion in great numbers, harried precinct workers provided

conflicting and apparently often inaccurate information to voters about

the ability or inability to correct spoiled ballots or other ballot

errors, and warnings regarding the confusing ballot situation failed to

even reach all affected precincts, among other obvious problems. These

problems occurred all through election day in Palm Beach County. The

statistically anomalous results of the voting in that area regarding

votes received by the Reform Party candidate Pat Buchanan would appear to

further validate this analysis -- the dramatic vote skew observed clearly

does not result from "normal" voting errors that can be reasonably

discounted or ignored.

Unlike the typical error rate expected in most elections where significant quantities of voter complaints are not received, the Palm

Beach situation, with its extremely atypical and alarming set of complaints and problems throughout election day, would appear to put those votes in a category that cannot be simply swept under the rug, and that appear to be deserving of immediate redress, adjustment, and/or revoting. These widespread voting problems in Palm Beach County were clearly not the fault of "inept" or "moronic" elderly voters, as some persons have arrogantly suggested.

3) Attempts to short-circuit the process of correcting the injustices and technical problems discussed above, through calls for rapid "closure" or the simple accepting of inaccurate and unjust results (particularly in Palm Beach County) "for the sake of the country" should be rejected.

We should not attempt to resolve this situation through quick "solutions" or calls for concessions. These same issues would be present even if the candidates' current positions were reversed. The critical questions shouldn't even be focused on the candidates at all, but rather on the VOTERS themselves, who appear to have been shortchanged by technical issues, procedural problems not under their control, and now by attempts by politicians to hurriedly dispose of this mess through vague references to the public good -- a route that would leave the affected voters effectively disenfranchised.

There are two efforts that need to take place. First, the problems of this

particular election, as discussed above, need to be dealt with in a deliberate and fair fashion. If that involves courts, manual recounts, and revoting, both inside and perhaps outside Florida, so be it -- they're all part of the procedures that we have in place. Let's get it right -- we should not be treating voters as disposable peons. If we do not take a proper course, whoever ends up in the White House will be viewed by at least half of the U.S. population, and probably much of the world, as not wholly legitimate.

Secondly, we need to look long and hard at the election process around this country, taking note that calls for radical departures from current widely-used systems must be viewed with extreme care and skepticism. In particular, Internet voting must be considered to be extremely problematic (please see the PFIR Statement on Internet Voting - <http://www.pfir.org/statements/voting>, and "Hacking the Vote" - <http://www.vortex.com/reality/2000-11-08>). One major reason to look skeptically upon these hi-tech systems is that their potential reduction in voter privacy and lack of rigorous audit trails fail to allow true recounts to occur when the integrity of the voting process is called into question, and such questions can arise in electronic as well as mechanical voting environments.

We stand at a crossroads where the existence of fundamental flaws in our election system have finally been exposed to the public. It is no longer tenable for the powers that be, with a gentleman's agreement or

a nod and a  
wink, to steamroll over these flaws -- and the will of voters --  
for the sake  
of convenience and expediency. We can start down the path  
toward ensuring  
genuine fairness and integrity in the voting process by making  
sure that the  
election of last Tuesday is resolved in a manner that not only  
serves the  
candidates, but more importantly the will of the voters  
themselves.

= = = =

Lauren Weinstein

lauren@pfir.org

(818) 225-2800

Co-Founder, PFIR - People For Internet Responsibility - [http://  
www.pfir.org](http://www.pfir.org)

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

Member, ACM Committee on Computers and Public Policy

Peter G. Neumann

neumann@pfir.org

(650) 859-2375

Co-Founder, PFIR - People For Internet Responsibility - [http://  
www.pfir.org](http://www.pfir.org)

Moderator, RISKS Forum - <http://catless.ncl.ac.uk/Risks>

Chairman, ACM Committee on Computers and Public Policy

<http://www.csl.sri.com/neumann>

---

## **Statement by Don A. Dillman on Palm Beach County Florida Ballot**

Rob Kling <kling@INDIANA.EDU>

*Fri, 10 Nov 2000 16:49:44 -0500*

Statement by Don A. Dillman on Palm Beach County Florida Ballot  
November 9, 2000

Several people have asked for my opinion on whether the format of the November 7, 2000, general election ballot in Palm Beach County, Florida, resulted in more people voting for Buchanan than had intended to do so. This statement is in response to those requests.

I cannot say with certainty whether the format of this ballot affected a certain number of people who thus voted by mistake for Pat Buchanan, while intending to vote for another candidate. That would require knowledge of what specific people did in the voting booth Tuesday, which I don't have. However, based on my experiences and past research concerning how the visual format of questionnaires affects respondents to surveys, I believe it is likely that certain visual features of the ballot resulted in some individuals who wished to vote for Gore inadvertently punching the second hole in the column, thus resulting in a vote for Buchanan. These visual attributes may also have resulted in double punches as people attempted to correct their error. However, I do not think that voters who intended to vote for Bush were similarly affected.

I believe this outcome occurred because of the joint effects of several undesirable features of the Palm Beach County ballot, rather than a single attribute. These factors include: (1) the listing of some candidates for President on the left-hand page of the ballot, while others were listed in a

separate group on the right-hand page; (2) use of a single column of circles between the pages to register one's vote, regardless of which page contained the candidate's name; (3) the lack of familiarity some people may have had with how to answer a punch ballot printed in this format; (4) the likelihood that most people knew which candidate they wanted to vote for prior to seeing any of the choices on the ballot; (5) the location of the presidential choices on the first pages of the ballot; and (6) the visual process people typically follow when registering preferences on a survey questionnaire or election ballot when it is unnecessary to read all choices (names of presidential candidates, for example) before registering one's vote. In order to mark their ballot, it was necessary for people to insert their paper ballot underneath the booklet that showed the ballot choices. They were then required to use a stick-pin answering device to punch through a circle on the ballot to make a hole in the paper ballot.

When people open and/or begin to read material printed in a booklet format, they tend to look first at the left-hand page and focus their attention there. Because this is a ballot in which most people expect to vote on most or all of the choices, it is also likely that they would expect to answer the questions in order. It is therefore likely that many voters began reading the left-hand page without first looking at the second page and seeing what material was printed there. Thus, they may have been unaware that some of the candidates for president were listed on the opposite page.

Most people who completed the ballot knew who they wanted to vote for prior to reading the list of names. Thus, rather than attempting to read all of the answer possibilities before marking their choice, they simply looked for the name of the candidate for whom they wished to vote. The typical procedure would be to start at the top of the list and read downwards until the preferred candidate was found.

After reading the first candidate's name (Bush) on the left-hand page, people who wanted to vote for him should have been guided to the answer column by the number and an arrow. That circle was also the first (or top) circle in the answer column. It therefore seems quite unlikely that the voter would by-pass the first circle and mark the second circle, thereby voting for Buchanan, by mistake.

In contrast, people who wanted to vote for Gore, and had just seen Bush's name, would be expected to go straight down the page as they searched for Gore's name. After finding it, people are likely to have moved their fingers and thumb that held the stick-pin punching device to the appropriate punching location. It is likely that in the process of doing this some people (particularly those who are right-handed) did not see the number and arrow pointing to the appropriate answer circle because it was obscured by their hand. They may have also concluded that the second hole in the column was the correct one to punch, simply because Gore was the second candidate

on the page. Thus, both the locational feature (being second) and mechanics of answering seem likely to have worked together in a way that led some people to inadvertently punch the second hole (Buchanan choice) rather than the third hole (Gore choice).

The possibility that some circles in the column of possible answers applied to Buchanan (on the next page) is unlikely to have occurred to some respondents. It is most unusual for any ballot or questionnaire to list choices to the first page to the right of the names, while choices to the second page are listed to the left of the names, and in addition to have all of them listed in a single column. Therefore, I would expect that some respondents had no idea that any of the choices in the answer column applied to the next page instead of to the candidates on page one. This problem was accentuated by the presidential preference being listed on the first page of the ballot, before the respondent had figured out, through experience, exactly how the ballot worked.

It does seem likely that some respondents who marked the second circle would have noticed that it was not aligned with the Gore box in the same way as the first circle was aligned with the Bush box. However, among those who noticed the different alignment this feature may have been discounted, because of their having to link together physically separate components (the actual paper ballot and the booklet listing candidate names) and the association of the second circle in the column with the second

candidate  
(Gore) choice.

I would also expect that some ballots were double punched (Gore and Buchanan) as voters started to punch the second circle, realized they were making an error, and attempted to recover from it.

Despite the visual and mechanical problems that individually and jointly increase the likelihood that Gore preference voters unintentionally and unknowingly voted for Buchanan, the nature of the problem is such that it would not affect most voters. Most people are able to "figure-out" how to answer questions when they are presented in a visually inappropriate way, as was done in this situation. However, I am also confident that some Gore-preference voters would have made the error described above. At the same time, and for the reasons described above, Bush-preference voters were not likely to make the same mistake.

Don A. Dillman is the Thomas S. Foley Distinguished Professor of Government and Public Policy at Washington State University in Pullman, Washington.

The opinions expressed here are his own and should not be attributed to his employer, Washington State University, or to the American Association for Public Opinion Research, for which he now serves as Vice-President and President-Elect. Background on the theory and research that lead to the interpretations reported here are published in Chapter 3 of Dillman, Don A. 2000 Mail and Internet Surveys: The Tailored Design Method, New York: John

Wiley; and Jenkins, Cleo R. and Don A. Dillman 1997 "Towards a Theory of Self-Administered Questionnaire Design," Chapter 7 of Lyberg, Lars, et al., Survey Measurement and Process Quality, (pp.165-196,) New York: Wiley Interscience.

Don A. Dillman, Social and Economic Sciences Research Center and Departments of Sociology and Rural Sociology, Washington State University  
Pullman, WA 99164-4014 phone: 509-335-1511 fax: 509-335-0116  
e-mail: dillman@wsu.edu <http://survey.sesrc.wsu.edu/dillman/>

---

## ✶ Florida vote counts

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

*Fri, 10 Nov 2000 10:23:07 PST*

The recount in Florida presents another interesting lesson in risks in the election process.

\* The recount in Palm Beach County increased the totals for Gore (+751) and Bush (+108).

\* An entire precinct had been left uncounted. The ballots had been run through the card reader, but the operator had pressed CLEAR instead of SET.

(The recount gave Gore +368, Bush +23.)

\* In Deland, Volusia County, a disk glitch caused 16,000 votes to be subtracted from Gore and hundreds added to Bush in the original totals.

This was detected when 9,888 votes were noticed for the

## Socialist Workers

Party candidate, and a new disk was created. (The corrected results were Gore 193, Bush 22, Harris 8.)

\* The day after the election, an election worker discovered a sack of about 800 ballots in the back of his car that obviously had not been included in the official results.

\* Voting cards failed to fit properly in the slots of some voting machines in Osceola County, giving 300 votes to the Libertarian candidate (where only 100 Libertarian voters are registered). Misaligned card machines have long been a source of errors.

\* In Pinellas County, election workers were conducting a SECOND recount after the first recount gave Gore more than 400 new votes. Some cards that were thought to have been counted were not.

[Source: Democrats tell of problems at the polls across Florida, \*The New York Times\*, 10 Nov 2000, National Edition A24]

Punched cards are inherently subject to differences on successive recounts. Hanging chad is clearly a problem, and successive mechanical recounts normally change the results each time. Human inspection is typically necessary to resolve conflicts.

Although electronic voting systems reduce the mechanical uncertainty that sometimes makes recounts necessary in punched-card elections, they also introduce different uncertainties in the integrity of the election process, and particularly in the integrity of the computer systems.

Certainly,  
hanging chad problems, paper fatigue, and tampering with punch  
cards would  
disappear, and recounts would be unnecessary: votes could be  
tabulated only  
as originally entered. But many new problems are also  
introduced. The  
opportunities for accidents and fraud are transformed into  
different  
categories -- such as tampering with software development and  
operation.  
And the desire for voter privacy is fundamentally in conflict  
with any  
requirements for accountability (e.g., audit trails).

In the Florida case, we still have to wait for the absentee  
ballots, and any  
possible further recounts in other states.

---

## **⚡ The end of the Multics era**

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

*Wed, 8 Nov 2000 20:09:31 PST*

Now that the very last Multics system has been decommissioned  
(last month,  
the Canadian Department of National Defense 5-processor  
configuration in  
Halifax), I am reminded of the primary goals of Multics  
expressed in the  
1965 Fall Joint paper by Corbato' and Vyssotsky, in which nine  
major goals  
were stated (courtesy of a note from John Gintell):

- \* Convenient remote terminal use.
- \* Continuous operation analogous to power & telephone services.
- \* A wide range of system configurations, changeable without

system or  
user program reorganization.

- \* A highly reliable internal file system.
- \* Support for selective controlled information sharing.
- \* Hierarchical structures of information for system administration and decentralization of user activities.
- \* Support for a wide range of applications.
- \* Support for multiple programming environments & human interfaces.
- \* The ability to evolve the system with changes in technology and in user aspirations.

These principles became fundamental to the Multics development and operation for the 35 years from 1965 until 2000. They are still relevant today, and they are still not as widely observed as they should be. So, to commemorate the final resting place of Multics, it seems appropriate to reiterate them here.

For background, check out Tom Van Vleck's Multicians Web site:  
<http://www.multicians.org>

PGN

---

## **✶ Excessive bounce activity and lost messages**

"Peter G. Neumann" <neumann@csl.sri.com>  
*Fri, 10 Nov 2000 16:28:53 PST*

Excessive bouncemail activity from [RISKS-21.11](#) (despite the fact that I had just removed over one hundred apparently bad addresses in the previous days resulting from bounces on previous issues) apparently blew our mail system for a while. In addition, while trying to cope with the many hundred new bounces, I inadvertently deleted some RISKS messages received on 9 November; those that I know about included Ed Reid, Joyce Scrivner, John Mainwaring, Peter Campbell, Tim Panton, Peter Smith, and Richard Cochran, although there were undoubtedly others. Apologies.

PLEASE try to use majordomo to UNSUBSCRIBE from an address that is about to go away BEFORE it goes away. Also, please check the RISKS Web sites if you have not received a message for a very long time and fear that your subscription might have been terminated -- especially if your own mailer has had a long outage (in which case you may indeed have been removed). (I have not yet installed the majordomo automated list-pruning facility, concerned for risks of overaggressive removal.) 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 21: Issue 13**

**Sunday 3 December 2000**

## Contents

- [Perspective on election processes](#)  
[PGN](#)
- [A better election process?](#)  
[Dave Stringer-Calvert](#)
- [Australian Internet cable severed](#)  
[Dave Farber](#)
- [CIA secret chat room investigated](#)  
[PGN](#)
- [McAfee VirusScan update crashes Windows](#)  
[PGN](#)
- [Ticking time bomb in buffer overflow](#)  
[Jonathan Hayward](#)
- [Re: The end of the Multics era](#)  
[Tom Van Vleck](#)
- [I am glad about the quality of my driver's license photo](#)  
[Joel Garry](#)
- [Re: Engine cutouts](#)  
[Paul Nowak](#)
- [REVIEW: "Practical Firewalls", Terry William Ogletree](#)  
[Rob Slade](#)

• [Info on RISKS \(comp.risks\)](#)

---

## ✶ Perspective on election processes

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

*Sun, 3 Dec 2000 9:59:37 PST*

We have long noted in this forum and before that in the ACM Software Engineering Notes (which I created in 1976 and edited for 19 years, until succeeded by Will Tracz -- who has carried on the tradition) that there are very serious actual and potential problems in computer-related elections. The current issue of *\*The New Yorker\** (4 Dec 2000) begins with The Talk of the Town section by considering the current mess: ``But it is not as if we were without warning.'' The article notes the series of writings of David Burnham in *\*The New York Times\** in 1985 and Ronnie Dugger's long article in *\*The New Yorker\** issue dated 7 Nov 1988. The article notes that Dugger's 1988 article quotes Willis Ware, who has long been a wise observer:

There is probably a Chernobyl or a Three Mile Island waiting to happen in some election, just as a Richter 8 earthquake is waiting to happen in California.

Many people have been asleep at the wheel for too long. See the Election material on my Web site

<http://www.csl.sri.com/neumann>

for pointers to some of the collected RISKS-historical material,

especially

the Illustrative Risks section on Election Problems, a document in which

I have long cited Burnham's articles from \*The NY Times\*, 29 and 30 Jul, 4

and 21 Aug, and 18 Dec 1985. (I have already noted the 14% undervote for

the Senate race in Florida in 1988.) What we are experiencing now is not a

new problem. Unfortunately, it had not previously reached Chernobyl-like

proportions or surfaced in a close presidential election.

Nevertheless, the

process that is currently before us is finally forcing an examination of

many of the relevant issues. I hope that some of the more basic deeper

issues will not be ignored in trying to resolve the immediate issues. The

time has come for a serious reassessment of the entire process.

Apologies for the long gap since the appearance of [RISKS-21.12](#) on 11 Nov

2000. We have received an enormous amount of e-mail on this topic, although

some of it has been superseded by events, and some of it is too politically

motivated to include here. There are so many issues at the moment, such as

chad slots that have not been cleaned in many years, the causes of dimpled

punched cards, absentee ballot irregularities, the desirability of manual

recounts in Florida and New Mexico and elsewhere, etc., that we cannot begin

to enumerate them here. On the other hand, objectivity would seem to be

extremely desirable at this time.

Let me offer just a few suggestions:

\* In the UK, Canada, France, Germany, and many other places, ballots for

national elections consist of a single piece of paper with one candidate to be selected for one office. This is an extremely reliable process, is counted very quickly in a highly distributed fashion, and seldom challenged. Perhaps in the U.S., elections for the President should be considered a Federal function and conducted by a one-issue paper ballot, with all other election issues run by local jurisdiction in their own way, as is the case at present. Even in such a simple paper ballot, the challenges of avoiding fraud and accidents are significant, but by no means unsolvable. The reliability can indeed be greater than in all of the alternatives.

\* If ballots are to be recorded and counted electronically, some sort of nonforgeable, nonalterable, and nonbypassable audit record must exist to make electronic tampering and accidents infeasible. Of course, voter privacy also needs to be honored. No existing electronic systems have anything close to what might be considered adequate, and the election system developers (with proprietary closed-source code) do not seem eager to take the extra miles needed for greater integrity. Claims of integrity are not backed up by standard practice of secure systems (which itself is extraordinarily weak), and no one seems to be applying even the relatively minimal standards of the Generally Accepted System Security Principles <http://web.mit.edu/security/www/gassp1.html> or reasonable certification processes.

\* Voting by the Internet, even if only from well established polling places, is and will remain extraordinarily risky because of the inherent untrustworthiness of computer systems attached to the Internet and indeed the networking itself. It should not be recommended for use in the foreseeable future.

\* Fraud and accidents must be anticipated throughout the election process. Election systems must be designed, implemented, and operated as systems in the large, and the human interfaces (for voters, administrators, maintenance personnel, etc.) must be considered as integral parts of the system. Any system should have live checking for invalid ballots. This existed decades ago in lever machines, and is common in electronic systems. If punched cards survive after 2000, card systems could easily include a single precinct display device that checks for overvoted or otherwise invalid ballots and for undervoted ballots before they are deposited.

\* I previously noted the doctoral thesis work of Rebecca Mercuri. She has devoted an entire dissertation to the topic of election system integrity, and particularly the conflicts inherent with process integrity and voter ballot privacy. The thesis takes a broad system approach to voting security/integrity/reliability, and is in fact relevant in a much broader context. Highly recommended. For information, see her Web site:

<http://www.seas.upenn.edu/~mercuri/evote.html>

Rebecca also considers a proposal for an auditable paper trail of each

electronic ballot that is verified by each voter before leaving and

automatically deposited in a tamperproof receptacle. This is still not

enough, but is worth considering as one more integrity measure. (For

example, voters should not be allowed to photograph that record, because

of the requirement that votes must not be salable, for example based on

paper evidence of how you voted!)

Many wags have cited the aphorism that perfection is the enemy of the good.

In election systems, there will never be perfection. But the existing state

of the art is the enemy of sanity, and a rush to all-electronic voting is

utter madness -- even though it may appeal to advocates of conceptual

simplicity. It is by no means an easy path, if all of the desired

requirements of the voting process are to be satisfied. And there is an

enormous gap between the concept and an implementation that provides any

real assurances.

[weak week typo fixed PGN]

---

## **A better election process?**

Dave Stringer-Calvert <dave\_sc@csl.sri.com>

*Fri, 01 Dec 2000 13:39:28 -0800*

If the election is not decided by the beginning of April 2001, then next time let's take inspiration from the lottery -- lottery 'turn out' is much higher than in elections, and there is already a large investment in the necessary infrastructure at your local 7-11 to handle it.

Pay to vote. Pay \$1 to cast a vote (we suggest voting early, and often).

Note that, for the lazy voter, the machines already have a 'random pick' function, if you have difficulty deciding on a candidate for yourself.

The collected monies are placed in a large fund which is either:

a) distributed to the 'winners' of the election (winner := people who voted for the winning candidate);

b) distributed to the 'losers' (loser := NOT winner), to compensate them for living under an administration they did not choose;

Of course, this would imply a tracking system in order to distribute the 'prize fund', violating the principles of anonymity of voting. So let's turn this upside down and offer a more effective use of campaign funds -- pay the voters who turn out, say \$5 each. They could use this to play the 'real' lottery, and perhaps by voting next year, you could win enough to run for presidential office in 2004...

Dave (who doesn't have the right to vote anywhere, but can still play the lottery)

## **⚡ Australian Internet cable severed**

Dave Farber <farber@cis.upenn.edu>

*Tue, 21 Nov 2000 21:05:35 -0500*

[PGN-ed from Dave Farber's IP.]

Australia's largest international Internet cable was severed on 20 Nov 2000

<<http://www.it.fairfax.com.au/breaking/20001121/A25-2000Nov21.html>> ,

partially disrupting Internet traffic in Singapore, Indonesia and Australia. The cable, carries about 60 percent of Australian ISP Telstra's

international Web traffic. While Telstra has since managed to <<http://www0.mercurycenter.com/svtech/news/breaking/merc/docs/026478.htm>>

redirect most of its Internet traffic to another undersea cable, bringing its

Internet services back to around 75 percent of capacity, its not yet been

able to determine how long it will take for Internet traffic across the

cable to return to normal.

[For Dave's archives and subscription information, see

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

. PGN]

---

## **⚡ CIA secret chat room investigated**

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

*Mon, 13 Nov 2000 08:16:29 -0500*

Following onto but totally unrelated to the John Deutch saga ([RISKS-20.78](#)),

the CIA has uncovered a secret chat room within its classified confines ``to trade off-color jokes, musings, and observations that went undetected for more than five years'' -- involving about 160 employees.

[Source: URL: <http://www.zdnet.com/zdnn/stories/news/0,4586,2652732,00.html>,

CIA secret chat room investigated, Tabassum Zakaria, Reuters, 12 Nov 2000, initially reported by \*The Washington Post\* on 12 Nov 2000. PGN-ed]

[Typo in 20.78 fixed in archive copy. PGN]

---

## ⚡ McAfee VirusScan update crashes Windows

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

*Sun, 3 Dec 2000 10:11:16 PST*

Windows 95, 98, and NT all seem to have crashed under McAfee virus definition file version 4.0.4102. It includes a driver that actually imitates the virus. Network Associates recommended starting in Safe Mode and disabling VirusScan's startup scan.

[Only 4102 versions? Be sure to subscribe to the virus-a-day club.]

---

## ⚡ Ticking time bomb in buffer overflow

Jonathan Hayward <jshayward@pobox.com>

*Wed, 22 Nov 2000 14:27:19 -0600*

A couple of months ago, a buffer overflow vulnerability was discovered in Outlook Express that allows arbitrary code to be executed when the user downloads messages with mauled date headers.

MicroSoft has released a patch that many people consider a cure worse than the disease. They still have yet to release a patch that users won't curse.

The Morris Internet worm hit the Internet at a time when there was no money to be made on it by insider trading.

Am I the only one to see a time bomb here?

-Jonathan

---

## **✶ Re: The end of the Multics era**

Tom Van Vleck <thvv@multicians.org>

*Sun, 12 Nov 2000 11:06:30 -0500*

Multics's ideas and approach to problem solving continue to be relevant. Those who had the privilege to work with the system and its team remember the experience fondly and apply its many lessons to new challenges. As I have written elsewhere, "as long as we have Multicians, we have the best part of Multics." Let's all use what we learned, and do some more work we can be proud of.

Incidentally, the 9 goals are in "Multics -- the First Seven

Years" by

Corbato/Clingen/Saltzer, 1972 FJCC, available on the Multicians website,

<http://www.multicians.org/f7y.html>

---

## **✶ I am glad about the quality of my driver's license photo**

Joel Garry <[joel\\_garry@compuserve.com](mailto:joel_garry@compuserve.com)>

*Sat, 11 Nov 2000 14:02:05 -0500*

The following is a paragraph from an article on [www.uniontrib.com](http://www.uniontrib.com) entitled

"Convention for chiefs of police displays crime-fighting tools," about The

International Association of Chiefs of Police having their convention in San Diego:

Also on display will be the RangeFinder, a facial recognition system that

is supposed to be able to scan everyone from people seated in cars to

those standing at a public gathering and automatically identify them from

data in government computer files. It is touted as capable of making

allowances for changes in appearance of the people it scans, such as

through aging, hairstyle alteration and weight gain or loss, said Mike

Maloney, a spokesman for NEC.

Unfortunately NEC doesn't seem to have posted details of this yet on the

website I checked (<http://www.nectech.com>, which does have details about a

fingerprint device mentioned in the article). However, it seems to me there

would be a risk of extrapolation error, as well as pattern matching variance issues. Beyond that, the differential between what humans perceive and what a technological device observes has already proved challenging to the legal system, and there is certainly a risk of believing the computer over people, as well as criminals modifying their behavior to fool the technology. I can't help but wonder how much of this technology relies on "image enhancement," where the algorithms employed may even have a net effect of supporting discredited theories of physiognomy.

[http://ourworld.compuserve.com/homepages/joel\\_garry](http://ourworld.compuserve.com/homepages/joel_garry)

---

## ✶ Re: Engine cutouts (Colburn, [RISKS-21.10](#))

Paul Nowak - SUPCRTX <pnowak@superiorcourt.maricopa.gov>

*Fri, 1 Dec 2000 18:01:16 -0700*

I got a kick out of this one having done the same thing with my 1990 Nissan 300zx when I first purchased it. My girlfriend lived in Pittsburgh, and between there and DC was a stretch of road that got over a steep ridge by means of a traverse. This naturally left little room for the Bear to set up and was the perfect place to test out my new wheels. I was carefully watching tach and speed so I would know the capabilities and handling of the car. Unfortunately I was unaware that there was an engine cutout and thought I had blown my engine. I just coasted down (I know how to drive

with the  
power assist gone...just keep the key at "ON" to avoid the  
little difficulty  
of the steering column lock) and \*very\* tentively re-started.

The real risk is not advertising \*all\* the safety features.

Paul(N)

---

## 🔥REVIEW: "Practical Firewalls", Terry William Ogletree

Rob Slade <rslade@sprint.ca>

Mon, 20 Nov 2000 14:56:51 -0800

BKPRCFRW.RVW 20000823

"Practical Firewalls", Terry William Ogletree, 2000, 0-7897-2416-2,

U\$34.99/C\$52.95/UK#25.50

%A Terry William Ogletree ogletree@bellsouth.net two@twoinc.com

%C 201 W. 103rd Street, Indianapolis, IN 46290

%D 2000

%G 0-7897-2416-2

%I Macmillan Computer Publishing (MCP)

%O U\$34.99/C\$52.95/UK#25.50 800-858-7674 www.mcp.com info@mcp.com

%P 491 p.

%T "Practical Firewalls"

Unfortunately, not much of this book is really practical. And a lot of it is not about firewalls, either.

Part one presents the fundamentals of understanding firewalls and security.

Chapter one looks at firewall basics, mentioning many topics but doing a poor job of explanation. Since the material is very generic there is almost

no detail. The TCP/IP content, in chapter two, is also quite vague, with lots of irrelevant details like DNS (Domain Name Service) record fieldnames, but little related to security, and that of low quality. Security and the Internet gives a general listing of threats, most not related to firewalls, in chapter three. Chapter four has some good discussion of some aspects of policy and design, but it is limited. There are rough outlines of firewalls structures, but the material on pros and cons is poor. (As the book progresses there are increasing amounts of repetitious text, as this chapter amply demonstrates.) The review of packet filtering, in chapter five, has some good points, but too much of the text relies on "one size fits all" pronouncements. Again, there is a lot of irrelevant detail on TCP/IP headers and not much on, say, filtering rules. Because a bastion host is very highly secured itself, chapter six is merely general security material, touching on too many operating systems for good coverage. Some good points but limited scope makes the proxy server topic weak in chapter seven. Chapter eight does slightly better on auditing, by limiting itself to UNIX and Windows NT.

Part two looks at encryption, the relationship of which to firewalls is problematic. Chapter nine does not really cover encryption technology, being simply a set of definitions of basic terms. Since a Virtual Private Network (VPN) is defined, in chapter ten, in terms of tunneling, the material is necessarily restricted to that subsection of the

field. Chapter eleven does not really tell the reader how to use PGP (the Pretty Good Privacy encryption program) but only deals with some aspects of installation.

Part three touches on installation and configuration of a number of products. Chapter twelve lists a number of firewall related tools, for UNIX, that are available on the Internet. "Lists" is definitely the operative word: so little information is given about the programs that chapters thirteen through sixteen cover basic installation and components of TCP Wrappers, TIS (Trusted Information Systems) Firewall Toolkit, SOCKS, and SQUID. ipfwadm and ipchains (for Linux) are described in chapter seventeen. Turning to Windows NT, chapter eighteen recounts the installation of Microsoft Proxy Server and nineteen does the same with the Elron CommandView firewall. Firewall appliances, or standalone units are promoted in chapter twenty. Chapter twenty one closes off with the same kind of vagueness and generalities given in part one.

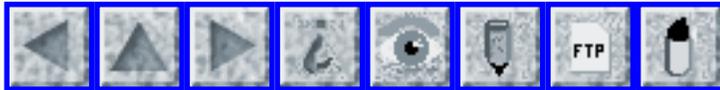
The most valuable part of this book is part three: even though the material is very limited, it is, at least, of some practical use. Most of the other content is of questionable accuracy or completeness, and therefore restricted in practicality. As noted, large sections of the text aren't even about firewalls. This book definitely does not compare with the classics like Cheswick and Bellovin's "Firewalls and Internet Security" (cf. BKFRINSC.RVW) or Chapman and Zwicky's "Building Internet

Firewalls"

(cf. BKBUINFI.RVW): a few suggestions about installation of specific programs does not make up for a lack of explanation of fundamental concepts, attacks, and defensive strategies.

copyright Robert M. Slade, 2000 BKPRCFRW.RVW 20000823  
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 21: Issue 14**

**Tuesday 12 December 2000**

## Contents

- [Internet and Electronic Voting](#)  
[PGN Rebecca Mercuri Lauren Weinstein](#)
  - [Re: Perspective on election processes](#)  
[Ben Laurie](#)
  - [Arizona Motor Vehicle counterfeiting rings](#)  
[Paul Nowak](#)
  - [Seattle Hospital Hacked](#)  
[Lauren Gelman](#)
  - [A new Chinook inquiry?](#)  
[Mike Ellims](#)
  - [Another Osprey crash](#)  
[PGN](#)
  - [Space Station risks](#)  
[Ben Hines](#)
  - [comp.risks considered harmful -- by some](#)  
[Thomas Roessler](#)
  - [REVIEW: "Hack Proofing Your Network", Ryan Russell et al.](#)  
[Rob Slade](#)
  - [Info on RISKS \(comp.risks\)](#)
-

## **IP: Internet and Electronic Voting**

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

*Tue, 12 Dec 2000 17:30:56 PST*

[Reproduced from Dave Farber's IP distribution,  
Date: Tue, 12 Dec 2000 20:36:19 -0500.]

A recurring mantra heard from some entities involved in the development and promotion of Internet-based voting systems is that they have conducted "public tests" and thus their systems are secure. If hackers don't break into such systems, the tests are declared a success.

This is of course illogical on its face, because it seems unlikely that people (both U.S. and internationally based) with an interest in subverting the U.S. election process would care to tip their hands by participating in what are essentially publicity stunts. These might attract your average 12-year old hacker, but not the pros who wait for production systems for their carefully mounted attacks.

In fact, using such "tests" as any sort of validation technique runs contrary to long-established computer and engineering verification practices, and makes a mockery of the rigorous design and testing that is required of systems that are to be deemed secure through extensive and methodical processes (e.g., to gain certification under the ISO Common Criteria or its predecessors TCSEC/ITSEC). "I left my Porsche out in the

parking lot with the doors unlocked and the key in the ignition and since it doesn't appear to have been stolen this must be a safe neighborhood," would be an equally nonsensical statement of supposed validation. All proposed voting systems should be subjected to rigorous evaluation, public inspection, and \*open-source code\* license agreements. Some applicable methodologies do exist, but have not been required. For example, Level 4 Common Criteria should be a \*minimum\* standard, although even that is not enough.

Security is only as strong as its weakest links. Internet voting (I-voting) will \*always\* be limited in its integrity by factors beyond the I-voting algorithms. For example, encryption can be an important part of an overall election system. However, although we have strong cryptographic algorithms, we do not have systems with adequate security into which the cryptography can be embedded. Furthermore, voter authentication, vote integrity, voter anonymity, auditability, accountability, recountability, and so on, are all involved, and many of these requirements operate at cross-purposes with one another. The massive vulnerabilities of standard personal-computer operating systems represent very serious concerns, in terms of hidden viruses, worms, Trojan horses, and further surprises unknowingly downloaded by the user with other packages, and waiting to pounce on election day. One proposed solution would be to boot a fresh system from external media in order to vote, but even such an approach does not adequately address these

potential vulnerabilities.

Deficient network protocols and the opportunities for insider fraud and accidental misuse abound. In addition to the issues noted above are the weaknesses that result from inadequate operational environments. Neither the client nor the server systems will be adequately secure under foreseeable technology -- including Internet Service Providers and Web servers. For example, proposals such as the use of rotating IP numbers and multiple systems to try to defend against denial of service attacks can be rendered impotent by similar attacks on network concentration points.

As always in any election environment, there are many opportunities for fraud, mischief, and manipulation -- despite ostensible checks and balances. These problems are exacerbated with electronic and Internet voting, where the lack of any physical ballots makes such manipulations impossible to detect and correct -- because there is no meaningful recount capability. Extraordinary vigilance is necessary, but never sufficient.

In the wake of the recent Presidential election problems, the knee-jerk reaction of "gee, can't we modernize and solve all this with electronic and/or Internet voting?" is predictable, but still wrongheaded. The shining lure of these "hype-tech" voting schemes is only a technological fool's gold that will create new problems far more intractable than those they claim to solve.

Peter Neumann, Rebecca Mercuri, and Lauren Weinstein

-----

Peter Neumann moderates the ACM Risks Forum, Chairs the ACM Committee

on Computers and Public Policy, and is a cofounder of PFIR -- People For Internet Responsibility <<http://www.pfir.org>>.

Rebecca Mercuri is a Professor of Computer Science at Bryn Mawr College.

She has provided expert testimony on voting systems throughout the past

decade. For information on her Penn doctoral thesis and other writings

on this subject, see <http://www.notablesoftware.com> .

Lauren Weinstein <[lauren@vortex.com](mailto:lauren@vortex.com)> and <[lauren@pfir.org](mailto:lauren@pfir.org)> moderates the

Privacy Forum <<http://www.vortex.com>> and is a cofounder of PFIR -- People

For Internet Responsibility <<http://www.pfir.org>>, and Member of the ACM

Committee on Computers and Public Policy.

Information on the Common Criteria is at

<http://csrc.nist.gov/cc>

An earlier statement on I-voting is at

<http://www.pfir.org/statements/voting>

---

## **Re: Perspective on election processes ([RISKS-21.13](#))**

Ben Laurie <[ben@algroup.co.uk](mailto:ben@algroup.co.uk)>

*Tue, 12 Dec 2000 13:17:26 +0000*

[From Dave Farber's IP]

> >Date: Sun, 10 Dec 2000 10:19:54 -0800

> >From: Ed Gerck <[egerck@safevote.com](mailto:egerck@safevote.com)>

> >  
> > Dave Farber wrote:  
> >  
> > > Date: Sun, 3 Dec 2000 9:59:37 PST  
> > > From: "Peter G. Neumann" <neumann@csl.sri.com>  
> > > Subject: Perspective on election processes  
> > > >  
> > > > .....

> > > > \* Voting by the Internet, even if only from well  
established polling  
> > > > places, is and will remain extraordinarily risky  
because of the  
> > inherent  
> > > > untrustworthiness of computer systems attached to the  
Internet and  
> > > > indeed the networking itself. It should not be  
recommended for use  
> > > > in the foreseeable future.  
> > > >  
> >  
> > The concern is justified but Peter ignores that there is a  
hacker-proof way  
> > to make an Internet-connected computer as secure as a non-  
connected one.  
> > The method was made public in its details and fire tested in  
a week-long  
> > 24-hour-a-day open attack test -- as reported in USA Today,  
Wired, and  
> > in <http://www.safevote.com/tech.htm>

"Hacker-proof"? Get real - cracker-resistant, perhaps, but  
what's new?

Safevote has a number of "snake oil" warning signs, including:

a) Use of multiple protocols: "in a real election Safevote would  
not  
know which algorithm is being used for encryption at any  
precinct",  
which is actually a rather silly claim - someone must know, or  
it would  
not be possible to decrypt - but ignoring that point, use of  
multiple  
algorithms merely adds a few bits to the keysize. Since there

are not  
that many algorithms that are actually any good, this really is  
very few  
bits.

b) Use of proprietary algorithms (DVC and friends).

c) Mysterious claims of the properties of a small number of bits  
("Each  
DVC also contains independent, multiple secure communication  
channels  
such as the voter's password, the ballot style to be used by the  
voter,  
and an internal secret.", yet they are only 30 bits long!).

d) "Cracking test" without disclosure of algorithms ("The  
specifications  
for Safevote's products and services under the Multi-Party  
technology  
will be made fully public and documented with open protocols,  
protected  
by flexible intellectual property rights that allow free non-  
commercial  
use." [note use of future tense]).

e) Existence of this "hacker-proof" technology brought to our  
attention  
by the owner - without bothering to mention this fact.

Of course, it could be great, but at this stage there's no way  
to tell.

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

---

## **Arizona Motor Vehicle counterfeiting rings**

Paul Nowak - SUPCRTX <[pnowak@superiorcourt.maricopa.gov](mailto:pnowak@superiorcourt.maricopa.gov)>  
*Tue, 5 Dec 2000 15:48:29 -0700*

[In the wake of voting irregularities, we have this another license fraud case. Surprised? PGN]

Thus far, 14 people have been indicted -- including four AZ Motor Vehicle Division customer service employees and an Arizona Department of Transportation computer information worker. Several more arrests are expected, with more arrests expected. Four groups are accused of issuing bogus licenses and ID cards, at a cost over \$1000 each. "Buyers apparently included criminals, illegal immigrants and motorists with suspended or revoked licenses." [Source: Article by Senta Scarborough, \*The Arizona Republic\*, 25 Nov 2000]

---

 Lauren Gelman <gelman@EFF.ORG>

Wed, 6 Dec 2000 19:26:05 -0500

Subject: Seattle Hospital Hacked

<http://www.securityfocus.com/news/122>

Seattle Hospital Hacked

Dutch hacker downloads thousands of patient records.

By Kevin Poulsen

December 6, 2000 3:54 PM PT

A sophisticated hacker took command of large portions of the University of Washington Medical Center's internal network earlier this year, and downloaded computerized admissions records for four thousand

heart  
patients, SecurityFocus.com has learned.

The intrusions began in June, and continued until at least mid-July, before network administrators at the Seattle teaching hospital detected the hacker and cut him off. The medical center was purportedly unaware that patient records were downloaded, and elected not to notify law enforcement agencies of the intrusions.

"It's a story of great incompetence," said the hacker, a 25-year-old Dutch man who calls himself "Kane." "All the data taken from these computers was taken over the Internet. All the machines were exposed without any firewalls of any kind."

SecurityFocus.com reviewed portions of the databases the hacker downloaded. One of the files catalogs the name, address, birth date, social security number, height and weight of over four thousand cardiology patients, along with each medical procedure they underwent. Another file provides similar information on seven hundred physical rehabilitation patients. A third file chronicles every admission, discharge and transfer within the hospital during a five-month period.

"I can say we're investing an incident," said hospital spokesperson Walter Neary. "We are taking it very seriously."

In a telephone interview, Kane said he did not tamper with any hospital data, and described his forays into the hospital's network as a renegade public service aimed at exposing the poor security surrounding medical

information.

A self-described computer security consultant by trade, the hacker's illicit investigation was inspired by a conversation with a colleague, in which they wondered aloud about how well highly sensitive computers were protected.

"The conversation came around to medical data, which is sensitive indeed, and I thought I'd have a look around," said Kane. <...>

Lauren Gelman, Director of Public Policy, Electronic Frontier Foundation

1-202/487-0420 <gelman@eff.org>

---

## **⚡ A new Chinook inquiry?**

Mike Ellims <mike.ellims@potechnology.com>

*Mon, 4 Dec 2000 10:08:58 -0000*

This is an update on an earlier series of postings. Apparently efforts to have a new inquiry into the Chinook crash on the Mull of Kintyre have been vetoed by the UK government.

The BBC quotes the public accounts committee report as saying that "there were repeated problems with the aircraft and the pilots should be exonerated" and that "the refit process was flawed".

Full story at,

[http://news.bbc.co.uk/hi/english/uk/scotland/newsid\\_1047000/1047469.stm](http://news.bbc.co.uk/hi/english/uk/scotland/newsid_1047000/1047469.stm)

In an earlier news item they report that in an earlier incident with another Chinook where no one was killed they report that there are

"documents

showing that Boeing, the helicopter's manufacturer, had agreed with software contractors that the FADEC was the cause of the 1989 accident and that the system needed to be redesigned".

Full story at,

[http://news.bbc.co.uk/hi/english/uk/scotland/newsid\\_821000/821274.stm](http://news.bbc.co.uk/hi/english/uk/scotland/newsid_821000/821274.stm)

Mike Ellims

Pi Technology

mike.ellims@pitechnology.com

www.pitechnology.com

phone +44 (0)1223 203 913 (direct)

phone +44 (0)1223 441 434 (reception)

---

## **✶ Another Osprey crash**

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

*Tue, 12 Dec 2000 08:39:41 -0800 (PST)*

Four Marines were killed on 11 Dec 2000 in North Carolina when another

experimental MV-22 Osprey tilt-rotor aircraft crashed. The remaining eight

Ospreys have been grounded, pending review by an expert panel. This

followed the loss of 19 Marines in Arizona in the spring 2000.

[Source:

PGN-ed from <http://abcnews.go.com/sections/us/DailyNews/osprey001212.html>]

---

## **✶ Space Station risks**

Ben Hines <bhines@san.rr.com>

Wed, 6 Dec 2000 01:15:01 -0800

Jim Oberg has written a great article in November's \*IEEE SPECTRUM\* discussing many risk issues and failure modes discovered during the recent space station missions.

It can be found here:

<http://www.spectrum.ieee.org/publicfeature/nov00/spac.html>

Ben <<http://tunnels.tripod.com/>>

---

## **⚡ comp.risks considered harmful (by some)**

Thomas Roessler <roessler@does-not-exist.org>

Fri, 8 Dec 2000 14:25:34 +0100

This site: <<http://sethf.com/anticensorware/smartfilter/gotalist.php>> lists

some results from a reverse-engineering effort against the black list used

by "SmartFilter". Apparently, comp.risks is being blocked by that software

under the "Criminal Skills" category, as are comp.dcom.telecom, comp.org.cpsr.announce, comp.org.eff.news, comp.protocols.tcp-ip, comp.security.announce, and others.

---

## **⚡ REVIEW: "Hack Proofing Your Network", Ryan Russell et al**

"Rob Slade, doting grandpa of Ryan and Trevor" <rslade@sprint.ca>

Mon, 4 Dec 2000 08:16:41 -0800

BKHPYNIT.RVW 20000831

"Hack Proofing Your Network", Ryan Russell et al, 2000, 1-928994-15-6,

U\$49.95/C\$77.50/UK#31.95

%E Ryan Russell

%E Stace Cunningham

%C 800 Hingham Street, Rockland, MA 02370

%D 2000

%G 1-928994-15-6

%I Syngress Media, Inc.

%O U\$49.95/C\$77.50/UK#31.95 781-681-5151 fax: 781-681-3585

%O www.syngress.com amy@syngress.com

%P 450 p.

%T "Hack Proofing Your Network: Internet Tradecraft"

According to the introduction, this book will teach you how to hack, or break into computer systems. With the best of intentions, of course. As it states, if you don't hack your system, who will? The intent is to teach you how to approach security breaking, with a view to finding, and then patching, the holes in your network.

Being an educator, and fairly cynical about anyone who tells me something is "safe," I have a lot of sympathy for this position. In theory. The implementation, though, may leave something to be desired. After all, those who are charged with protecting systems generally have other things to do. They have limited resources. They don't have a lot of leisure, or interest, in testing every single piece of software for any possible buffer overflow condition. So security managers may not be all that interested in spending all of their non-existent free time obsessively hacking their own systems.

Well, having reviewed the book, and sent off the draft, the lead author, Ryan Russell, informed me that security managers were not the real intended audience. This work was actually aimed at the keeners, those few who \*do\* really want to get behind the user interface, and poke about in the workings. But it may have some use beyond that rather select crowd. In Russell's own words, this is what you do after you've got good policies in place, and you've got your routine down for applying patches, watching for new vulnerability announcements, and so forth.

Part one, rather oddly entitled "Theory and Ideals," seems to concentrate on basic concepts. It also may seem strange that chapter one, called "Politics," starts out by defining "hacker" and other related terms. On the other hand, any text that tries to argue for the social value of criminals and frauds is bound to be considered political. Ultimately, this piece seems to be trying to justify system breaking activities. All the usual arguments are trotted out, and make the normal amount of sense (very little). (I should also point out that this book started life as an electronic text. This is evident in the frequent citations of Web sites in the course of the work. They may support the content in the context of a Web page, but in print they are annoying, since the relevant material is not incorporated into the book.) Chapter two, "Security Laws," is more a set of cliches: what can go wrong will go wrong, security by obscurity doesn't work. Some of them are wrong (passwords can be securely stored with one-way encryption, albeit still at some risk of brute force attacks; and the NSA has goofed on an algorithm), some are naive

(the assertion that there is no guaranteed protection against viruses makes no mention of Fred Cohen's work), and most are of questionable utility. The classes of attack listed in chapter three are neither comprehensive nor fully explained. (Most of the space in the chapter is given over to source listings of attack tools.) "Methodologies" seems to be a collection of random thoughts on analysis in chapter four.

Part two describes some activities intended to be undertaken on a computer over which you have complete control, mostly related to decryption. Chapter five looks at making small changes to a system, and checking for modifications. This is a useful function in any kind of analysis, but the examples chosen will hardly be of use to sysadmins. The author admits that chapter six really does not explain cryptography, it really only mentions some password cracking tools. Both chapters seven and eight essentially deal with bad data, first in general terms and then in the specific problem of buffer overflows. While the discussion might be of interest to programmers, it is of limited use to security managers.

Part three talks about attacks on remote systems. There is a little explanation about sniffing (which requires some level of local access), session hijacking, and spoofing. Chapters twelve and thirteen list some security holes in server and client software respectively. Oddly, given all the problems in earlier parts of the book, the material on viruses and malware, in chapter fourteen, isn't too bad. It's not great, it displays too much virus code to very

little effect, and has a few holes, but it is generally better than the stuff found in standard security texts, and stands out above the rest of the book.

Part four contains a single chapter. Although the titular subject is reporting, most of the material promotes the concept of "full disclosure." This is the tenet that security is best served by having all security loopholes disclosed. The discussion does take a fairly responsible tack, recommending that vendors be contacted first, and allowed some time to fix the problem, before the vulnerability or exploit is released to the public. The text is fairly reasonable, although it does contain the full text of a number of email exchanges which add little to the debate. The remaining pages concentrate on the importance of continual study in the security field.

The people who have contributed to this book are a step above the usual "wannabes" who tend to write "hacker" security books. The information presented is also somewhat more reliable, and covers a broader range. However, both the thesis and the execution of the work contain flaws. The material still seems more interested in justifying security breaking expeditions than in giving the security administrator a complete and useful reference for protection. Errors, while less rampant than in other, similar texts, are still too common for the content to be considered really dependable. In particular, basic concepts are too quickly dismissed in the eagerness to pass along news of the latest "cool tool." Experienced security managers may find some helpful recent data in this volume, but probably

already

have resources of their own. Newcomers to the field are advised not to rely too heavily on this as a single source of knowledge.

As noted, though, the authors were not really writing for managers or novices. For software engineers, programmers, and testers, there is possibly more utility. Those doing sophisticated software evaluations, and particularly those with sufficient resources to really "test to destruction," might get the most out of the book, especially considering the concentration on breaking, rather than fixing. Still, some research in the RISKS and BUGTRAQ archives would likely get you just as much.

copyright Robert M. Slade, 2000 BKHPYNIT.RVW 20000831  
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 21: Issue 15**

**Weds 20 December 2000**

## Contents

- [Wells Fargo computer network outage](#)  
[PGN](#)
- [ATM network for voting: a non-starter](#)  
[David Jefferson](#)
- [Re: Voting by machine](#)  
[Fred Cohen](#)
- [Alaska Airlines flight 261](#)  
[Jim Horning](#)
- [NY State DMV canceling auto registrations](#)  
[Danny Burstein](#)
- [Another DMV Break-in, in Oregon](#)  
[PGN](#)
- [Healthcare data bank contains inaccurate and flawed information](#)  
[Mike Beims](#)
- [Germany to rely on on-board diagnostics for vehicle emission checks](#)  
[Bernd Felsche](#)
- [High reliability](#)  
[Adam Shostack](#)
- [Electrocution leads to more deaths](#)  
[Martin Minow](#)

- [Spam as a denial of service attack?](#)  
[Steve Bellovin](#)
  - [Re: Seattle Hospital Hacked](#)  
[Lynda Ellis](#)
  - [Computers, Freedom, and Privacy CFP2001 Call for Participation](#)  
[HIIP](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

## ⚡ **Wells Fargo computer network outage**

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

*Sun, 3 Dec 2000 21:12:02 PST*

On 1 Dec 2000, the nationwide Wells Fargo computer network crashed for a few hours, three days after WF had finished merging their computer networks with those of Norwest (which bought WF in 1998). One of four Hitachi Tritium 400 mainframes in the Minneapolis data center shut itself down, apparently after detecting some sort of anomaly. The result stopped all banking operations that depend on real-time interaction. [Source: Article by Sam Zuckerman, \*San Francisco Chronicle\*, 2 Dec 2000, PGN-ed]

---

## ⚡ **ATM network for voting: a non-starter**

David Jefferson <jefferson@pa.dec.com>

*Tue, 19 Dec 2000 20:34:40 -0800 (PST)*

The suggestion to use the inter-bank ATM (automated teller machine) networks

for voting in public elections has been floated in several places recently. From a purely hardware point of view, the ATM network has some very desirable security properties: It is a private, national-scale network, unconnected to the Internet, and thus not subject to Internet-based attacks. The terminals are hardened, and are often equipped with cameras and other security devices for remote monitoring, and hence are resistant to tampering (as befits machines carrying tens of thousands of dollars in cash). They are very rugged and reliable. Many have touch-screens, which allows about the simplest possible human interface.

However, in a number of other ways the ATM network is not appropriate for voting. The first problem has to do with voter privacy, coercion, and vote selling. When a person votes in a private situation (i. e. other than a public polling place) there is opportunity either for the voter to be coerced, or to sell his/her vote. Although we live with this fact for absentee ballots, it is not a good idea to give up entirely on the strongest election security and privacy measure ever invented: the Australian secret ballot system in which people are required to vote alone in the privacy of the voting booth, with public observers to assure that no one accompanies them to influence them.

A related issue is voter authentication. It is not sufficient to simply issue voters ID cards with magnetic stripes so they can authenticate themselves using the ATM machine's bank card reader. This is a

clear

case where the requirements for voter authentication are much stronger than that for financial transactions. People are entitled to authorize someone else to use their ATM card, since it is common for people to share access to money accounts. But a voter authentication system must prevent such sharing, even with a trusted person or a spouse, since the right to vote is nontransferable. Furthermore, unfortunately, voter ID cards and PINs can also be sold, opening the door to widespread vote selling. Stronger authentication than the presentation of a card and PIN must be required when there are no election clerks around to take voters' hand signatures (which can be checked against registration records).

By far the greatest concerns, though, with the possible use of the ATM network for voting, are reliability and security. Even assuming we have confidence in our ability to design and build reliable, secure distributed systems in general (a false assumption), an additional fundamental problem arises in contemplating voting over the ATM network: an irresolvable conflict in the need to run two independent secure systems (the election system and the ATM banking system) on the same networked platform at the same time.

An absolute requirement for the reliability and security of any voting system is for election officials to control ALL of the hardware, software, and networking of all clients and servers, including the operating systems

on the voting terminals. (This is the same argument showing why remote Internet voting is today so hopelessly insecure.)

An exactly symmetric argument applies, of course, from the bankers' point of view: the security of the ATM system also rests on the fact that they control ALL of the hardware, software, and networking of their platforms.

If one tried to run both systems on the same terminals and network concurrently, then either the banking software could act like a giant Trojan horse inserted into the election system, or vice-versa. Election officials would worry (rightly) that bank employees or contractors might insert code to undermine the election; and banking officials would worry (rightly) that election administrators or vendors would insert code to steal money! Or the presence of either system might degrade the reliability or performance of the other. It is a practical impossibility to prove that the combined system has no bad interactions, and in general it is just not hopeless to run two mutually-distrusting, mission-critical, high security systems on the same network platform. The situation is made even worse (if that is possible) by the fact that ATM software is totally proprietary; and unless the principle of public source software is established for elections, the same will be true for election software.

The bottom line, then, is that in order to permit secure voting over the ATM network, the (many) network owners would have to be willing

to turn  
it over entirely to election officials for the duration of the  
election.  
Since, quite reasonably, the owners are not about to do that  
even for  
one day, let alone for enough time to build, test, debug, and  
certify  
such a system, the suggestion to use the ATM network for voting  
is a complete  
nonstarter.

David Jefferson, Compaq Systems Research Center, Palo Alto, CA

---

## ✶ Re: Voting by machine

Fred Cohen <fc@all.net>

*Wed, 13 Dec 2000 05:09:05 -0800 (PST)*

In order for any practical election process to really gain  
assured  
trust, it must have several properties:

- 1) It must be sufficiently simple and open so that the  
average  
person on the street can clearly see exactly how it  
works,  
understand it clearly and fully, and participate in it.
- 2) It must be observable by all parties at all times so  
that  
there can be no real question about its legitimacy that  
cannot  
be answered by the individuals who were present at the  
scene.
- 3) It must produce evidence that cannot be easily  
altered or  
destroyed, that can be judged by non-experts examining  
it, and

that is not separate from the actual vote - they must be one and the same.

4) It must be very inexpensive to purchase, maintain, and operate.

The lifecycle cost must be on the order of pennies per vote or less and it must be easily maintained by untrained people.

5) It must not depend on anything outside itself to operate, like electrical power, telephone lines, servers, etc.

6) There must not be significant spoilage of supplies or recorded results - either before or after the fact.

7) It must be physically securable on a local basis by local officials and police officials.

8) Each voting location must be able to function independently of all others in every vital aspect of the operation other than the summarizing of overall votes that cross localities.

9) Each voting location must be able to have unique vote layouts and candidates to accommodate the wide range of elections that run both simultaneously and sequentially.

10) The voters must believe that the systems works.

At this point in time, and for the foreseeable future, computerized and particularly Internet-based voting machines and networked voting systems do not, and will not, fulfill the majority of these requirements.

1) They are far too complex and full of details for the

average

person on the street can understand at all.

2) The vote goes into a mystery thing and comes out somewhere else

as a total. Nobody at the scene sees it go in or come out.

3) The evidence they produce is easily altered and destroyed and it

requires substantial expertise to even view any evidence it leaves.

Furthermore, that evidence is not in any physical way linked to the

original vote.

4) They are expensive to purchase, maintain, and operate. The lifecycle cost is on the order of dollars per vote and they

can only be properly maintained by experts.

5) They depend on electricity, network connections, servers, and so

forth.

6) There are no supplies (except power and hardware components that

require maintenance and replacement) but spoilage cannot universally

be detected.

7) The votes not physically securable on a local basis by local

officials and police officials because the system is networked.

8) Each voting location can not function independently of others.

9) Each voting location can have unique vote layouts and candidates

10) I don't believe that the systems work, but most

voters may be  
fooled into that belief by a sufficient perception  
management  
process.

Fred Cohen at Sandia National Laboratories at tel:925-294-2087  
fax:925-294-1225

Fred Cohen & Associates: <http://all.net> - fc@all.net - tel/  
fax:925-454-0171

Fred Cohen - Practitioner in Residence - The University of  
New Haven

---

## **✈ Alaska Airlines flight 261**

Jim Horning <horning@intertrust.com>  
*Tue, 19 Dec 2000 10:47:48 -0800*

[FW: Not a computer risk so much as a systemic risk, but  
interesting. JH]

AVflash                      Vol. 6, Issue 51a                      Monday, December  
18, 2000

The Top Headlines From AVweb's Expanded, Illustrated News  
Coverage at

<<http://avweb.com/n/?51a>>.

ALASKA AIRLINES FLIGHT 261: THE HEARINGS...

In the aftermath of the January 31 crash of Flight 261, where an  
Alaska

Airlines MD-80 plunged uncontrollably into the Pacific Ocean  
after failure

of part of the aircraft's stabilizer assembly, the NTSB is  
uncovering some

of the shortcomings of a number of systems currently in place.

We found out

last week, through official FAA testimony, that the jackscrew  
assembly (a

1960s design) has outlived its paper trail. FAA officials testified that they could not provide an account of how the part was approved -- nor could they provide records of the process which approved it. So, what we are left with is a part with some 35 years of flight history, but not a single official record or word on how it came to be approved for installation in the MD-80.

...WHAT WE KNOW, NOW...

While the design of the jackscrew assembly was supposed to assure that the failure of any single part within the assembly can \*not\* result in complete loss of control, the crash of Flight 261 explains with relative certainty that the failure of a single part \*is\* capable of causing failure of other parts in the assembly and that those multiple failures are quite capable of bringing down the aircraft. Further, while the manufacturer was aware that the assembly was subject to continuous wear, they were content in the notion that regular maintenance could assure its operation. Alaska Airlines was inspecting the jackscrews every 15 months, but the accident aircraft had flown 8,874 hours since its last inspection -- well beyond the 7,200 suggested by Boeing. The hearings revealed that the FAA had "accepted" the carrier's jackscrew maintenance schedule.

...AND WHAT THE CREW SAID, THEN

The pilots radioed their Seattle base seeking advice and relaying their understanding of the serious nature of the situation. Portions of the communication that were made public last week indicate that the

base

operators were not immediately aware of the magnitude of the problem. This may have induced some agitation in the cockpit as ground-based counterparts second-guessed the captain's decision to divert to LAX and the problem proved its ability to overcome each sequence of corrective measures set forth by the flight crew. During the aircraft's final dive, the verbal exchange between the pilots appears to imply that they attempted to stabilize the aircraft in inverted flight and work with its gyrations to help them roll it back over and keep the nose near the horizon with rudder and elevator inputs. But all attempts by the crew to regain control proved futile as the MD-80 made its final plunge to the ocean.

[PGN-ed: Article in \*The New York Times\* 18 Dec 2000 noted by Kevin Ziese,

who observed that

"Had the system operators realized that parts replacement is itself a

critical computing function, it's possible that safeguards would have

been in place to generate the appropriate alert in a more timely manner.

This underscores the importance of recognizing 'critical computing'

requirements in all organizations. Even though the system may not be

man critical, it may have a significant impact on safety. Integrated

systems, especially in a network-centric world, need better safeguards

and control mechanisms than the typical software developer provides." ]

## **NY State DMV canceling auto registrations**

danny burstein <dannyb@panix.com>

*Mon, 11 Dec 2000 03:29:36 -0500 (EST)*

The New York State Department of Motor Vehicles (DMV) has a new computer system that is supposed to help locate uninsured motorists, based on information provided electronically by insurance companies. Unfortunately, the database includes drivers who are apparently properly insured -- and who are very unhappy when they are arrested even if they are carrying valid proof-of-insurance cards. The DMV blames drivers for not responding to mailed warnings, although it certainly does not appear blameless, based on the frequency of complaints. [Source, Ann L. Kim, Insurance Is No Insurance Against State DMV Glitch \*Newsday\*, 10 Dec 2000; PGN-ed]

---

## **Another DMV Break-in, in Oregon**

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

*Sun, 18 Dec 2000 22:00:11 PST*

On the heels of Paul Nowak's [RISKS-21.14](#) report of the Arizona Motor Vehicle counterfeiting rings came this somewhat belated report of a break-in at the Gresham, Oregon DMV office on 12 Dec 2000. The thieves were apparently pretty well prepared, as they took less than two minutes to take computer

equipment containing personal information on 3,215 people who had recently obtained licenses, plus blank cards and a machine for making bogus drivers' licenses and ID cards. [Source: Stuart Tomlinson, \*The Oregonian\*; PGN-ed. Was at [http://www.oregonlive.com/news/oregonian/metroeast\\_week.ssf](http://www.oregonlive.com/news/oregonian/metroeast_week.ssf) ?/news/oregonian/00/12/metroeast/e6\_dmv15.frame]

---

## **✶ Healthcare data bank contains inaccurate and flawed information**

Mike Beims <mbeims@mail-fair.ivv.nasa.gov>  
*Mon, 11 Dec 2000 10:01:55 -0500*

From Reuters and Medscape (Reuters Health), 1 Dec 2000:

"The US government's warehouse of disciplinary records and malpractice actions against physicians and other healthcare practitioners is incomplete and inaccurate in many cases, congressional investigators conclude in a new report."

<http://managedcare.medscape.com/reuters/prof/2000/12/12.04/20001201legi001.html>

The National Practitioner Data Bank is considered by this report to be seriously flawed and raises a red flag regarding patient privacy.

Like other data banks mentioned in the Risks Digest, when used to track social issues such as credit, criminal activity, and driving records, these data banks can be useless and possibly dangerous to everyone

involved.

Mike Beims <Mike.A.Beims@ivv.nasa.gov>

---

## **Germany to rely on on-board diagnostics for vehicle emission checks**

Bernd Felsche <bernie@innovative.iinet.net.au>

*Thu, 14 Dec 2000 09:46:38 +0800 (WST)*

\*Auto Motor und Sport\*, 8 Dec 2000, [a motoring magazine published in

Germany] reports that the emissions compliance inspection of new vehicles

will be performed solely by reading the ODB (on-board diagnostic) codes.

The "testing" regime is to commence no later than July 1st, 2001.

All new gasoline-engined cars are already equipped with OBD, according to

DEKRA [a company which performs vehicle inspections] and all diesel-engined cars from 2003.

ODB is a self-checking function of engine management systems that

determines whether there are excessive deviations in exhaust emissions

[amongst other factors] by checking plausibility and correlation with

other sensors. A check-engine warning usually alerts drivers of a problem

with various sensors and actuators.

Emission checks can also be performed simply by reading stored error codes

from OBD, specifically if the lambda sensor(s) [aka O2 sensor] functions

correctly and if the catalytic converter is still converting sufficiently.

The simplified "check" is expected to reduce inspection costs to motorists; by some 70 to 80 German Marks according to DEKRA.

[Loose translation by Bernd from <http://www.autouniversum.de>, PGN-ed]

Regular RISKS readers might observe that there are would longer be any external checks to verify that the system is actually doing what it reports.

Bernd Felsche - Innovative Reckoning, Perth, Western Australia

---

## ⚡ High reliability

Adam Shostack <adam@zeroknowledge.com>  
*Mon, 4 Dec 2000 13:51:20 -0500*

An article on a new center to study high reliability computing <http://www0.mercurycenter.com/svtech/news/indepth/docs/nasa120300.htm>

contains this text:

```
> current practices in the semiconductor industry. Both are
> enormously
> complex processes, but the semiconductor industry has figured
> out a
> way to produce chips with relatively few errors -- at least in
> comparison to the software industry, which typically has from
> 6 to
> 30 errors per line of code.
```

Not to mention the journalism industry, with an error rate of 1 error per 6

to 30 bits when reporting technical information... :)

---

## **⚡ Electrocuting leads to more deaths**

Martin Minow <minow@pobox.com>

*Mon, 18 Dec 2000 23:49:48 -0800*

Two teenagers were electrocuted by "an energized streetlight."  
After the electrocution, the county ordered all streetlights extinguished until they could be rewired. Then, a man was struck and killed by a car while crossing the darkened street and a motorist killed in a two-car collision in the same area. [Summarized by Martin Minow, minow@pobox.com]  
<<http://www.miamiherald.com/content/today/news/dade/digdocs/062954.htm>>

Quoting from the article:

Some residents complained Sunday that the precautionary order by the county to turn off the 92 streetlights has made matters worse. Now passing motorists see only with the illumination from their headlights. ... It's unclear how long the maintenance work on the streetlights will take, Miami-Dade spokeswoman Rhonda Barnett said.

[When will they see the light in Miami-Dade? PGN]

---

## **⚡ Spam as a denial of service attack?**

Steve Bellovin <smb@research.att.com>

Sun, 10 Dec 2000 09:47:13 -0800

According to the AP, Verizon was bombarded by millions of spam messages, slowing e-mail to its dial-up customers. Verizon believes that "it was a malicious attack".

--Steve Bellovin

[Doneel Edelson cited \*InformationWeek\*, 18-25 Dec 2000, page 37:

<<http://www.informationweek.com/817/verizon.htm>>

That article notes that 70,000 subscribers had delays up to several hours,

and this was the \*third\* spam attack against Verizon in two weeks. PGN]

---

## ✶ Re: Seattle Hospital Hacked ([RISKS-21.14](#))

"Lynda Ellis (LabMed)" <lynda@mail.ahc.umn.edu>

Wed, 13 Dec 2000 10:52:10 -0600 (CST)

Here's the response from the University of Washington, Health Sciences and Medical Affairs, News and Community Relations, 7 Dec 2000

The following statement is for attribution to Tom Martin, director and chief information officer for University of Washington Medical Centers Information Systems:

An Internet-based news service yesterday netcast a rumor that 'a hacker took command of large portions of the University of Washington

## Medical

Centers internal network earlier this year.' Unfortunately, this rumor was reported as fact. However, it is completely inaccurate.

Last summer, we halted an unknown hacker who had gained criminal entry into portions of our academic computer system. This is the only incident we are aware of that bears any resemblance whatsoever to the report in yesterdays SecurityFocus News. While we have no evidence that confidential data were obtained as part of that incident, we do know for certain that no one has ever gained unauthorized entry into our separate and highly confidential patient-care computer systems.

The UW and most other universities make limited use of firewall technology and are under constant assault by recreational hackers. Recognizing this, we take extraordinary measures to protect our clinical-based systems that go well beyond the high security employed, for example, by most community hospitals. These measures include the latest hardware and software, encryption technologies, and strong host-based security.

As the incident we detected last summer illustrates, we are constantly vigilant for hacker attacks on all of our computer systems. We believe that rumors such as the one given credence in yesterdays netcast only encourage recreational hackers to pursue their criminal activity."

For more information, contact L.G. Blanchard or Walter Neary, 1-206-543-3620

## **✦ Computers, Freedom, and Privacy CFP2001 Call for Participation**

<HIIP@Harvard.edu>

*Fri, 15 Dec 2000 14:37:45 -0500*

CFP2001: The Eleventh Conference on Computers, Freedom and Privacy

Hyatt Regency Cambridge  
Cambridge, Massachusetts, USA  
March 6 - 9, 2001

### CALL FOR PROPOSALS

The Program Committee of the Conference on Computers, Freedom, and Privacy (CFP2001) invites your participation and proposals for the eleventh annual CFP, which will be held at the Hyatt Regency in Cambridge, Massachusetts, USA, on March 6 - 9, 2001.

CFP2001 is sponsored by the Association for Computing Machinery (ACM).

CFP is the leading policy conference for exploring the impact of the Internet, computers and communications technologies on society. For more than a decade, CFP has anticipated the policy trends and issues and shaped the public debate on the future of privacy and freedom in the online world. Each year at CFP, key members of the technical, government, business, education, non-profit, legal, law enforcement, security, media and hacker/cracker communities gather together to address the

cutting edge

questions in computing, freedom and privacy. CFP themes are broad and forward-looking. CFP explores what will be, not what has been.

Since this CFP will be held in 2001, the theme is the future of computing, freedom and privacy, including the convergence of information and communication technologies with other advanced technology areas and the new challenges to freedom and privacy that they engender throughout the world.

The Internet is a global phenomenon with significant local impacts. We encourage innovative and imaginative thinking on these topics and invite you to submit proposals for CFP2001 conference activities. Of particular interest are proposals on:

GOVERNANCE, including impact of the Internet on governance; impact of governance on the Internet; ICANN; voting; standards; antitrust and competition policy; new models for governance; and stakeholders in governance.

SOCIAL IMPACTS, such as the relationship between the individual and her communities.

INDIVIDUAL AUTONOMY AND INTEGRITY, particularly human rights; freedom of expression; censorship; free speech and access; freedom of association; freedom of movement; and exploration of the roles of non-identifiability, pseudonymity, and anonymity.

CONVERGENCE of information and communication technologies (ICT); of ICT and content; of ICT with other advanced technology areas, including

biotechnology, biology and materials science; and related industry mergers, consolidations and activities.

DIGITAL DIVIDE in the face of the growth of the ubiquitous information environment; access to the network infrastructure; access to information; broadband policy; education policy; and related telecommunications, cable, intellectual property and freedom of information (FOIA) rules.

PRIVACY, including the growth and role of the chief privacy officer; privacy as the default; US legislation; international developments and trends; and an international privacy convention.

INTERNATIONAL ISSUES, especially the emerging issues of global privacy protection; international principles of human rights; security of information systems; intellectual property; objectionable content; cybercrime; jurisdiction; regulation; and legislation.

ELECTRONIC COMMERCE, including consumer protection; and the impact of payment systems, regulations, and technical standards on personal freedom and privacy.

We encourage proposals not only on these subjects, but also on the border areas between these topics, such as intellectual property protection and privacy.

We strongly encourage proposals that involve leading experts, innovators, policymakers, and thinkers.

CFP2001 PROPOSAL SUBMISSION GUIDELINES

Proposals should be submitted no later than January 5, 2001, via the CFP2001 website at <http://www.cfp2001.org>.

Proposals should include the following information:

1. PRESENTATION TITLE

2. PRESENTATION TYPE

Plenary conference sessions (30 minutes to 1.5 hours)

Lunch breakout sessions (1 hour)

Tutorials (3 hours)

BOFs ("birds of a feather" sessions) (no time limit)

3. PROPOSED LENGTH OF PRESENTATION

4. NAME(S) OF SPEAKER(S), PLUS BRIEF BACKGROUND DESCRIPTION FOR EACH

SPEAKER

5. A BRIEF DESCRIPTION (no more than 100 words) OF THE TOPIC AND FORMAT,

suitable for conference brochure and press release.

6. COMPLETE CONTACT INFORMATION (e-mail, phone, and mailing address). For

presentations with more than one speaker, please include complete contact

information for all the proposed speakers.

We encourage a variety of formats, including panels, debates, individual

speeches or keynotes, interviews, role plays, reverse role plays, case

studies, Socratic dialogues, etc.

DEADLINE FOR SUBMISSION OF PROPOSALS

All proposals must be received no later than January 5, 2001.

Please

follow the submission guidelines above.

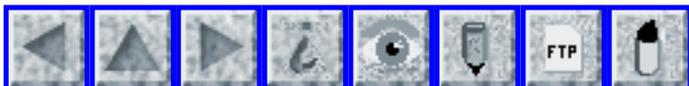
PLEASE SUBMIT PROPOSALS AT [HTTP://WWW.CFP2001.ORG](http://WWW.CFP2001.ORG).

For additional information about CFP2001, please visit the conference

website at <http://www.cfp2001org>.



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 21: Issue 16**

**Tuesday 26 December 2000**

## Contents

- [Power cut blocks emergency calls](#)  
[Stuart Lamble](#)
- [Important message from egghead.com CEO](#)  
[Egghead.com](#)
- [Security advisories becoming less open?](#)  
[Chris Adams](#)
- [Another tidbit about the new Microsoft advisory format](#)  
[Richard M. Smith via Brian](#)
- [Making something look hacked when it isn't](#)  
[Richard J. Barbalace](#)
- [The risk of a seldom-used URL syntax](#)  
[Rob Warnock](#)
- [Intelligence risks of e-mail auto-responses](#)  
[Dan Birchall](#)
- [Re: Voting by machine](#)  
[Tony Finch](#)
- [Re: ATM network for voting: a non-starter](#)  
[Jeremy Epstein](#)  
[Barry Margolin](#)  
[Bill Stewart](#)
- [Re: High Reliability](#)  
[Matt Jaffe](#)

- [Re: Another DMV Break-in, in Oregon](#)  
[Simson L. Garfinkel](#)
  - [Re: Seattle Hospital Hacked](#)  
[Todd Wallack](#)  
[Kevin L. Poulsen](#)  
[Jonathan Thornburg](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

## ⚡ Power cut blocks emergency calls

Stuart Lamble <Stuart.Lamble@lodbroker.com>

*Thu, 21 Dec 2000 09:49:46 +1100*

Excerpted from <http://www.theage.com.au/news/2000/12/21/FFX0NEBVXGC.html>

"Emergency lines went dead for six minutes shortly after 1am [on Wednesday, 20th December] until an emergency generator restored services. ... While no callers rang during the critical period, noone could have sought assistance had there been an emergency. ... In case of power failure, the call centres have a diesel generator. But Mr Bahr [technical representative for the Bureau of Emergency Services Telecommunications] said he was aware of an incident in the past when the back-up had failed."

---

## ⚡ IMPORTANT MESSAGE FROM EGGHEAD.COM CEO

"Egghead.com Special Update" <specialdeals@PROMO1.EGGHEADLIST.COM>

*Sat, 23 Dec 2000 09:43:41 -0800*

Dear Customer,

Egghead.com has discovered that a hacker has accessed our computer systems, potentially including our customer databases. While there is no indication that any customer information has been compromised, as a precautionary measure, we have taken immediate steps to protect you by contacting the credit card companies with whom we work. They are in the process of alerting card issuers and banks so that they can take the necessary steps to ensure the security of cardholders who may be affected.

We wish to underscore that we have taken these steps as precautions. We have no information at this time to suggest that any credit card information has been compromised. We are investigating this possibility, and we are doing everything we can to proactively protect you. If you would like further information, you may wish to contact the issuer of your credit card to determine what steps they are taking. We regret any inconvenience this may cause you.

We issued a press release on this matter earlier today. [...] If you have additional questions, please call our customer service team at 1-800-EGGHEAD (344-4323).

Respectfully,

Jeff Sheahan, President & CEO, Egghead.com, Inc.

[The Press Release notes that Egghead has "retained the world's leading computer security experts to conduct a thorough investigation of our security procedures and an analysis of this breach." PGN]

## ✂ Security advisories becoming less open?

"Chris Adams" <chris@improbable.org>

Tue, 12 Dec 2000 22:45:18 -0800

Recently there has been some discussion on BUGTRAQ regarding some companies attempts to change the way they publish security advisories.

Some background:

<http://www.securityportal.com/list-archive/bugtraq/2000/Dec/0036.html>

<http://www.securityportal.com/list-archive/bugtraq/2000/Dec/0042.html>

<http://www.securityportal.com/list-archive/bugtraq/2000/Dec/0056.html>

<http://www.securityportal.com/list-archive/bugtraq/2000/Dec/0054.html>

<http://www.securityportal.com/list-archive/bugtraq/2000/Dec/0076.html>

<http://www.securityportal.com/list-archive/bugtraq/2000/Dec/0101.html>

Basically, it started when Microsoft abruptly switched to a new advisory format where the notification e-mail included only a cursory description of the problem and a [malformed] URL for the actual report. Today, Elias Levy announced that @Stake wanted to switch to a format with more information in the message but still requiring a visit to their website for the full advisory.

Some interesting RISKS:

- Access for people with marginal Internet connections or browsers other than IE/Netscape is less convenient.

- Information is unavailable if the webserver is down or overloaded, as might happen with an important advisory. It seems counterproductive to put important, time-sensitive material behind a single point of failure, particularly when the decision is to deliberately avoid using a free

distributed, fault-tolerant distribution channel.

- It makes it much easier for a vendor to change an advisory without notifying anyone, especially since changed or removed advisories won't be archived in anywhere near as many places as a mailing list such as BUGTRAQ. In addition to covering up bad work, this would also make it easier to remove or tone-down past advisories about companies the author is now aligned with.
  
- It opens the prospect of tailoring content to the reader. This could be as simple (and annoying) as charging for access to some content or as complex as determining what to show based on where the request came from (e.g. competitors, vendors or journalists). While this would probably be caught for something major, particularly at first, it would not surprise me to find at least subtle tampering happening regularly if this becomes commonplace.

I find it hard to ignore the above concerns given that the switch provides no benefits of any sort to the reader, let alone enough benefit to outweigh them. The only legitimate advantage from such a policy is that it makes it easier for the author to change the contents of a released advisory. For legitimate purposes, this is unnecessary:

- Updates to current advisories can be published in the same fashion as the originals, ensuring that anyone who received the original will receive any updates.
  
- It's extremely easy to add a link to the advisory which people could use to check for updates.

- It discourages the use of proper change control, since it's easier to update an existing advisory than release a update.
- It will cause old links to break if they ever move content around and neglect to install a redirect for the old URL. (Microsoft is notorious for this, especially with links that break only for visitors using something other than Internet Explorer)

---

## 🔥 [BUGTRAQ] Another tidbit about the new Microsoft advisory format

Brian <ang\_mor@CAM.ORG>  
Fri, 08 Dec 2000 00:38:47 -0500

Now we are 'Bugged by Microsoft'. A nuisance. Brian

Date: [accidentally deleted]  
From: "Richard M. Smith" <rms@PRIVACYFOUNDATION.ORG>  
Subject: [BUGTRAQ] Another tidbit about the new Microsoft advisory format  
To: BUGTRAQ@SECURITYFOCUS.COM

One thing that I noticed about the new Microsoft security bulletins is that they now contain Web bugs. The bugs look like they are used to count the number of people coming to read the bulletins. Here is the URL for one of these bugs:

[http://c.microsoft.com/trans\\_pixel.asp?  
source=www&TYPE=Pv&p=technet\\_security\\_bulletin](http://c.microsoft.com/trans_pixel.asp?source=www&TYPE=Pv&p=technet_security_bulletin)

I didn't see a <IMG> tag for the bug, so I'm assuming it is generated by one of the JavaScript files included on the page.

One thing that Microsoft is learning here is what bulletins people consider important. With the older format, where all the info was in an e-

mail  
message, they did not get this feedback.

I don't see the use of Web bugs here as a big deal, but still interesting.

Richard

---

## ✂ Making something look hacked when it isn't

"Richard J. Barbalace" <rjbarbal@MIT.EDU>  
*Sat, 16 Dec 2000 15:03:27 -0500*

A brief e-mail has been getting forwarded around our campus which reads:

Check out breaking news at CNN:  
[http://www.cnn.com&story=breaking\\_news@18.69.0.44/evarady/www/top\\_story.htm](http://www.cnn.com&story=breaking_news@18.69.0.44/evarady/www/top_story.htm)

At first glance, this appears to be a genuine article on CNN, but a quick read reveals that a cute joke. Most people who have seen the fake article have immediately assumed that [www.cnn.com](http://www.cnn.com) has been hacked in some manner.

Those more familiar with HTTP specification, however, will notice that the URL is completely valid, and does not lead to or redirect from any [cnn.com](http://www.cnn.com) computers. No machines have been hacked. Instead, the e-mail just plays with your expectations of what a URL should look like. The risk here is not a computer one at all, but a social risk that even (or perhaps especially) knowledgeable people will assume something has been hacked when it hasn't been.

An even sneakier URL might be:

[http://www.cnn.com&story=breaking\\_news@306511916/evarady/www/top\\_story.htm](http://www.cnn.com&story=breaking_news@306511916/evarady/www/top_story.htm)

For those of you still pondering why that URL works, read the HTTP spec and try the equivalent:

[http://username@18.69.0.44/evarady/www/top\\_story.htm](http://username@18.69.0.44/evarady/www/top_story.htm)

Richard J. Barbalace <rjbarbal@mit.edu>

---

## ✶ The risk of a seldom-used URL syntax

Rob Warnock <rpw3@rigden.engr.sgi.com>

*Mon, 18 Dec 2000 21:09:19 -0800 (PST)*

Recently, a mailing list I'm on forwarded a report of a "hack" of the CNN.com site. Upon looking closely, I found that the CNN site hadn't been hacked at all -- it was the \*minds\* of readers of this hoax "report"

that were being hacked! Rather cute, actually, but it exposes what is perhaps a larger RISK, so please bear with me while I set up the story...

An MIT student named Eric Varady took a parody news article from The Onion <URL:[http://www.theonion.com/onion3637/bush\\_horrified.html](http://www.theonion.com/onion3637/bush_horrified.html)> ,

edited the layout to resemble CNN's format, and copied it to his own site

<URL:[http://salticus-peckhamae.mit.edu/evarady/www/top\\_story.htm](http://salticus-peckhamae.mit.edu/evarady/www/top_story.htm)> .

(Note that multiple threatened legal actions have since forced him to remove the original content, but an explanation page is still there.)

He then passed around a "report of a hack of the CNN site" with a URL [which I \*do\* hope makes it through the mail-to-HTML scripts at Catless!] of

<URL:[http://www.cnn.com&story=breaking\\_news@18.69.0.44/evarady/www/top\\_story.htm](http://www.cnn.com&story=breaking_news@18.69.0.44/evarady/www/top_story.htm)> .

If you look very closely, you'll see that the actual host named by

this URL

is not "www.cnn.com", but "18.69.0.44" (a.k.a. salticus-peckhamae.mit.edu).

That is, for IP-based/Internet URL "schemes" such as HTTP or FTP, the general format defined in RFC 1738 is:

```
<scheme>://[<user>[:<password>]@]<host>[:<port>]/<url-path>
```

The "user" field is very rarely used, and even then is more often seen with

FTP than HTTP. But since it contained an at-sign before the first slash,

the hoax URL was really <URL:[http://18.69.0.44/evarady/www/top\\_story.htm](http://18.69.0.44/evarady/www/top_story.htm)>

with the (ignored) user field of "www.cnn.com&story=breaking\_news". Cute, eh?

More serious scams of this sort are possible, given the number of users

who (1) have \*no\* idea what the formal syntax of a URL is, and (2) routinely

access the Web through "portals" which often create complicated indirection

URLs to aid with logging or tracking to support advertising revenue, e.g.:

```
<URL:http://www.foo.bar.com/logger.cgi?http://www.other.place.com/some\_article>
```

The RISK is that users are being bombarded with these monstrosities so

often that they've grown used to it, and that they'll fail to recognize

when they're being sent someplace they might not really want to go!!

(Perhaps when it's not a joke, such as being sent to a porn site while

working at a company with a "no tolerance" policy.)

---

## **✶ Intelligence risks of e-mail auto-responses**

Dan Birchall <djb0x77376989@scream.org>

20 Dec 2000 01:54:13 GMT

For some time, I have been associated with organizations that maintained e-mail lists for communication with customers. Each customer mailing generates some quantity of e-mail responses to the mailing address or a specified reply-to address. Heuristic filters handle the most frequent types of responses, generating automatic replies or redirecting mail to appropriate addresses. There are, though, always some messages which the filters can't adequately handle, so my involvement tends to involve eyeballing them.

The workload is by no means immense - for every 6,000 outbound messages sent, I manually handle one response. Some are questions the filters didn't catch, which I pipe to various scripts. Some are bounce messages. Some are chain letters - I grep those for From: headers and bounce them to the appropriate administrators; nothing to spread holiday cheer like a corporate policy smackdown. A good many are auto-responses.

Within the set of auto-responses, a significant minority pose non-technical risks. Users who are going to be "away from mail" or "out of the office" for even a single day frequently leave instructions on who should be contacted in their absence, and their responses often include other information that could be considered sensitive.

Their expectation is, of course, that they will receive mail from co-workers and colleagues who already know where they work, what they do, and have some need for the information. However, if they are subscribed to mailing lists, it is quite possible that the information they provide will be seen by completely unrelated users at other organizations.

"I will be away from [government laboratory] from [departure date]

and will return on [return date]. If you need to reach someone from the IT Security staff, Please contact [coworker] at [number] or e-mail to [address]."

Congratulations. You've just told me what department you work in and where you work (the combination of which might not be the sort of thing you don't just go blabbing around), and given me a co-worker's name and direct contact information. The potential for a social engineering hack is giddy.

This is, of course, a somewhat extreme example. But for each one like this, there are hundreds of others from people in business, academia and government. People who're perfectly willing to send total strangers information about their personal schedules - who they are, what they do, where they do it, when they're leaving, when they're coming back, where they're going, how they can be reached while they're gone, or who to contact instead.

Perfectly normal information to give to a co-worker, colleague or neighbor. Somewhat risky information to give to strangers, in an era of competitive intelligence, corporate and other espionage, etc.

Workarounds? You could hack your MTA/MUA/MDA to only send responses to certain domains, or omit all personal information from your auto-response.

A more balanced approach would involve not re-stating information authorized users already know, and delivering necessary information in a minimal form.

Ergo, instead of:

"I will be away from GovLab from December 22 and will return on December 26. If you need to reach someone from the IT Security staff, Please contact John Smith at 809-555-1212 or e-mail to jsmith@govlab.gov."

send something like this:

"I am currently away from work. If you need to reach someone, please contact John <jsmith> at 555-1212."

The logic, of course, is that an authorized person already knows where you work, what you do, your e-mail domain, and your area code. Nobody needs to know how long you'll be gone, if there's someone else who can help them.

Dan Birchall - Palolo Valley - Honolulu HI - [http://dan.scream.org/Corporate Holidays 2001](http://dan.scream.org/Corporate%20Holidays%202001) - <http://208.184.171.20/articles/262573.htm>

---

## ✶ Re: Voting by machine (Cohen, [RISKS-21.15](#))

Tony Finch <dot@dotat.at>

*Thu, 21 Dec 2000 21:12:22 +0000*

One of Fred Cohen's requirements for an election process to be deemed trustworthy was this:

> 9) Each voting location must be able to have unique vote layouts  
> and  
> candidates to accommodate the wide range of elections that run both  
> simultaneously and sequentially.

One of the aspects of the American election that is very strange to someone used to the British election process is that so many different votes are made on the same ballot paper. If one ballot paper is used for each vote then the counting process can be made much simpler, faster, and more reliable. The ballots can be quickly split into piles per candidate, and then those piles can be counted in parallel. Votes for different issues can also be counted in parallel. Separate "ambiguous" piles can be examined more

closely if necessary.

This also means that statewide elections can use the same ballot paper across the state without affecting the need for counties or cities to have their own ballots for their own elections.

Tony f.a.n.finch fanf@covalent.net dot@dotat.at

---

**✶Re: ATM network for voting: a non-starter (Jefferson, [RISKS-21.15](#))**

Jeremy Epstein <jepstein@monumental.com>

*Wed, 20 Dec 2000 17:50:23 -0500*

David Jefferson's well thought out critique of ATM-based voting misses one small but important point. Depending on where you live, it is not necessary to provide any authentication, or even to sign, in order to vote. Until this year, in Virginia all I had to do was state my name and address to the election official, and that was sufficient. Given the number of voters in each precinct (thousands in a presidential election), it's likely that I could have voted several times using a different (valid) name each time. If I knew the names and addresses of people in other precincts, I could therefore vote for them as well.

The law changed this year, and now you either have to present some form of picture ID, or you must sign an affidavit. But they don't have a signature to compare to at the voting booth, so in the best case they find out after the fact that \*someone\* voted illegally (but they can't tell which vote it was).

I mention this because all of the discussions about electronic voting (ATM-based, Internet-based, or otherwise) presuppose a requirement for strong authentication. If we're trying to model the paper world, that's not

necessarily so. [Recognizing, of course, that there's not enough time to vote 1000 times in the same day in the paper world, under the assumption that I'd have to rotate between precincts to escape detection, but I can certainly vote electronically 1000 times in the same day.]

Jeremy

---

**✉ Re: ATM network for voting: a non-starter (Jefferson, [RISKS-21.15](#))**

Barry Margolin <barmar@genuity.net>

*Wed, 20 Dec 2000 23:13:05 GMT*

>A related issue is voter authentication.

We've heard this mentioned repeatedly in discussions about online voting.

I don't know how voting works in your community, but there's virtually no authentication in my town. I go to the polling place, they ask me my name and address, and they cross it off the voter list; another person does the same thing when I turn in the completed ballot. None of the people there know me, yet they never ask for any proof of identity. A teenager trying to get into a bar at least has to have a fake ID; he wouldn't need that to vote as someone else -- all the information he needs is in the phone book.

However, if I tried to vote multiple times in the same precinct I suspect they would recognize me. So in order to stuff the ballot, I would have to go to different precincts, which would be quite tedious. With an electronic system, the door is opened to massive fraud by a single

individual.

Barry Margolin, barmar@genuity.net, Genuity, Burlington, MA

---

**✶ Re: ATM network for voting: a non-starter (Jefferson, [RISKS-21.15](#))**

Bill Stewart <bill.stewart@pobox.com>

*Thu, 21 Dec 2000 00:43:08 -0800*

There's only one positive feature to using the ATM network for voting, which is that you can pay bribes to voters right on the spot. Other than that, it's totally impractical - ATMs use common physical formats for cards and for currency, but they don't have common processors, programming environments, network protocols, or user interfaces, and the real interoperation is done by the host processors that feed the networks and common banking standards, not because there's any interoperation out at the edges.

Most of them use some variant on SNA, which was relatively appropriate technology at the time ATM networks started evolving, and are some variant on a PC - I've seen Dead-MSDOS messages on out-of-order ATMs, some have run OS/2, some Unix, while others probably have custom or other production operating systems.

Bill Stewart <bill.stewart@pobox.com>

---

**✶ Re: High Reliability (Shostack, [RISKS-21.15](#))**

Matt Jaffe <jaffem@pr.erau.edu>  
Thu, 21 Dec 2000 01:02:29 -0700

>> -- at least in comparison to the software industry, which typically  
>> has from 6 to 30 errors per line of code.

His (appropriately sardonic) comment was:

> Not to mention the journalism industry, with an error rate of 1 error  
> per 6 to 30 bits when reporting technical information... :)

My (equally sardonic) comment is about the original (hidden) assumption that one can somehow compare chip error rates with software error rates. I was not aware that there was a published conversion factor converting transistors to lines of code. Perhaps I'm using the wrong metric and it's errors per pound of silicon that can be converted somehow to an equivalent in errors per line of source code. In any case, I'll bet if we first converted lines-of-code to pixels-to-display-a-line-of-code, software and hardware error rates would start to look a lot more similar.

...Matt

<http://backoff.pr.erau.edu/jaffem>

---

## ✈ Re: Another DMV Break-in, in Oregon (PGN, [RISKS-21.15](#))

"Simson L. Garfinkel" <slg@walden.cambridge.ma.us>  
Wed, 20 Dec 2000 22:07:24 -0500

In the mid 1990s, Pitney-Bowes developed and demonstrated a system for digitally-signed drivers licenses. I believe that the system was called VERITAS, but I could be wrong. The system provided for a 2D barcode on the

back of each driver's license. The barcode contained a digitized copy of the driver's photograph, name, address, height, age, etc. The 2D barcode was signed with the digital key of the day, which itself was signed with the system key. I believe that the system key was changed every year.

The company's business plan, I believe, was to basically give away the identity systems to state governments and then to sell verifiers to stores, restaurants, bars, etc. You would slap a person's driver's license down onto the verifier and it would display their photograph and tell you if they were old enough to drink, etc. It would also verify the signature.

The Pitney-Bowes system was specifically designed to prevent the break-in-and-steal-it problem. Each morning the systems in the field would call up and get their key-of-the-day signs by the system-key. If a system was stolen, those systems wouldn't get signed. If they actually issued fraudulent cards, you could blacklist those cards and distribute the blacklist to the verifiers. You could even use caller ID to make sure that you wouldn't issue certs the phone number it was calling from wouldn't match the caller ID, and the system wouldn't issue a key.

I saw this system at the RSA conference in 1993 or 1994. I was quite impressed. But Pitney-Bowes never sold it. I believe that there was a patent infringement problem.

---

## ✶ **Re: Seattle Hospital Hacked ([RISKS-21.14,15](#))**

Todd Wallack <twallack@sfchronicle.com>

*Wed, 20 Dec 2000 15:36:12 -0800*

I just spoke to Walter Neary at the university of Washington. He confirmed a 9 Dec 2000 report in \*The Washington Post\* that hackers gained access to confidential medical files. He said it was a good summary of the incident. (Other newspapers and television stations also reported on the incident as well.)

But the statement you distributed was issued two days earlier. At that time, Neary said the college didn't know whether to believe the hackers' claims that they had accessed confidential data. He said the Washington Post and other reporters later obtained proof -- the records themselves -- that show that the hackers did indeed break into the computer.

But he still disputes an Internet report, referenced in the statement, which claims that hackers "took control" of the university's computers.

Todd R. Wallack, Business Reporter, San Francisco Chronicle  
(415) 764-2815

---

## ✶ Re: Seattle Hospital Hacked (Wallack, [RISKS-21.16](#))

"Kevin L. Poulsen" <klp@securityfocus.com>  
*Thu, 21 Dec 2000 17:43:04 -0800 (PST)*

\*The Washington Post\*, and a local TV station, obtained the "proof" from me, after the medical center sought to dismiss the incident as a rumor. Though I should hardly have to say it, I confirmed every aspect of this story before breaking it. (Even we "Internet reporters" do that sort of thing.)

The hacker took command of large portions of the medical center's internal network.

The University of Washington Medical Center later reluctantly acknowledged the accuracy of my report.

<http://www.washingtonpost.com/wp-dyn/articles/A46320-2000Dec8.html>

<http://www.nytimes.com/2000/12/08/technology/08HACK.html>

<http://www.msnbc.com/news/499856.asp>

[http://dailynews.yahoo.com/h/ap/20001208/us/med\\_center\\_hacker\\_3.html](http://dailynews.yahoo.com/h/ap/20001208/us/med_center_hacker_3.html)

<http://www.komotv.com/news/qtmovie.asp?ID=8157>

Kevin L. Poulsen, Editorial Director, SecurityFocus.com, Washington D.C.  
(202)232-5200

---

## ✦ Re: Seattle Hospital Hacked ([RISKS-21.14](#), [21-15](#))

Jonathan Thornburg <jthorn@galileo.thp.univie.ac.at>  
*Thu, 21 Dec 2000 18:24:12 +0100*

In [Risks 21.15](#), "Lynda Ellis (LabMed)" <lynda@mail.ahc.umn.edu> wrote  
> The following statement is for attribution to Tom Martin, director  
> and chief  
> information officer for University of Washington Medical Centers  
> Information  
> Systems:  
>  
[[...]]  
> we do know for certain that  
> no one has ever gained unauthorized entry into our separate and  
highly  
=====  
> confidential patient-care computer systems.

I find this highly implausible. I could perhaps accept a claim that these systems are very secure, but to say that no one has ever gained unauthorized entry strains credibility. How does Mr. Martin

know this? More to the point, how could anyone know this? In the real world, all software has bugs in it, and all systems have loopholes.

If nothing else, authorized users can be bribed, coerced, or fooled by "social engineering".

> we take extraordinary measures to protect our clinical-based systems that  
> go well beyond the high security employed, for example, by most community  
> hospitals. These measures include the latest hardware and software,

=====

> encryption technologies, and strong host-based security.

Using the "latest" hardware and software does not boost my confidence in "extraordinary" security.

Some of the RISKS here:

- \* Wildly over-optimistic claims like these suggest that (as usual) management is pretty clueless when it comes to computer security.
- \* Managers who actually believe the systems are perfect don't have much incentive to improve them, or even examine/audit them too closely...
- \* Line employees who might actually be very competent are more likely to quit when confronted with pointy-headed bosses.
- \* And oh yes, the UW statement was right: claiming "our systems have never had unauthorized access" probably does boost the chances of further attacks.

Jonathan Thornburg <jthorn@thp.univie.ac.at> Universitaet Wien / Institut fuer Theoretische Physik <http://www.thp.univie.ac.at/~jthorn/home.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 21: Issue 17**

**Tuesday 26 December 2000**

## Contents

- [Martin Minow](#)  
[PGN](#)
- [Australian Ansett B767 fleet grounded due to maintenance breaches](#)  
[Mike Martin](#)
- [Interference forces RAF to abandon ILS](#)  
[David Kennedy](#)
- [Risks of automatic firmware upgrades](#)  
[Marc Roessler](#)
- [IBM and Intel push copy protection into ordinary disk drives](#)  
[John Gilmore](#)
- [CERT's ActiveX security report](#)  
[Richard M. Smith](#)
- [Privacy/quality risks in Quicken Online Billing](#)  
[Clay Jackson](#)
- [Credit report lists ex-spouse's address](#)  
[Beth Roberts](#)
- [Wanna know my salary ?](#)  
[John C Haselsberger](#)
- [Re: Spam as a denial of service attack?](#)  
[Steve Wildstrom](#)

● [Armageddon scenario near-miss](#)

[Scott Rainey](#)

● [Info on RISKS \(comp.risks\)](#)

---

## ✶ **Martin Minow**

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

*Tue, 26 Dec 2000 15:18:39 PST*

It is with deep sadness that we note here the sudden passing of Martin Minow last Thursday. He was a long-standing, noble, insightful contributor to RISKS, dating back to Volume 1, number 33, on 1 Jan 1986. A quick search shows that he had 172 messages in RISKS over the past 15 years, including translations of some otherwise inaccessible news items that appeared in Swedish sources. He was a delightful person, and will be sorely missed by many of us. Thanks to all of you who forwarded the e-mail message from his brother, Robtminow@aol.com.

Greg Marriott <greg@spies.com> added URLs for Martin's Web pages:

<http://www.vmeng.com/minow/>

<http://homepage.mac.com/k6mam/>

<http://www.ag.ohio-state.edu/~natres/faculty/homepage.html>

PGN

---

## ✶ **Australian Ansett B767 fleet grounded due to maintenance breaches**

"mike martin" <bullarook@bigpond.com>

Sun, 24 Dec 2000 08:52:40 +1100

On 23 Dec 2000, Ansett Airlines, Australia's second national airline, grounded six of its fleet of seven B767-200 aircraft (its largest domestic aircraft) when "it realised that important maintenance inspections had not been carried out". (The seventh aircraft was already out of service for maintenance.) See

[http://www.abc.net.au/news/2000/12/item20001224050838\\_1.htm](http://www.abc.net.au/news/2000/12/item20001224050838_1.htm) and <http://www.smh.com.au/news/0012/24/national/national1.html>.

This, at perhaps the busiest travel weekend of the year, and when Ansett has been steadily losing market share to Qantas. Oddly enough, while this inconvenienced thousands of passengers, it was reported that only 18 flights were cancelled (what do these aircraft do all day then?).

It appears that a mandatory 25,000-cycle maintenance check was completely overlooked, but the good news (if true) is that an Ansett spokesperson was reported by the Australian ABC network as saying that "the decision to take the aircraft out of service was entirely [Ansett's] own". So, if there were risks introduced by cost cutting or other measures by management of Ansett, owners Air New Zealand, or part shareholder Singapore Airlines, the system corrected itself.

Albeit, likely with huge commercial pain. One Ansett customer was quoted by the \*Sun Herald\* Sunday newspaper as saying, "I haven't flown Ansett for 20 years and it's only now that I remember why."

<http://www.smh.com.au/news/0012/24/national/national2.html>

While there is no reason to consider that Australian airline travel is more risky than it used to be, the landing of a Qantas B747 in a Bangkok golf course last year

<http://www.theage.com.au/news/20000430/A31680-2000Apr29.html>

was the first of a number of breakdowns of types we have not hear about before. Earlier this year, the new Sydney Airport control tower was blacked out by electrical supply failures twice within a few days. The result was short term chaos.

Last week the control tower was evacuated due to smoke from burning computer equipment. However, backup procedures cut in quickly and the old control tower took over.

Conclusion?

Positive... I think.

It seems that maybe organisations are becoming more transparent about risks, and improving measures to deal with them. While passengers inconvenienced by the Ansett grounding might have a different view, it was, from the information publicly available, a brave decision.

Even so, the threads at [www.pprune.org](http://www.pprune.org) abound with contrary suspicions.

Neither the regulator, Civil Aviation Safety Authority Australia, nor the Australian Transport Safety Board has yet posted any comment on the event on their web sites.

We shall see.

Mike Martin, Sydney mike\_martin@altavista.net

---

## ✶ Interference forces RAF to abandon ILS

David Kennedy CISSP <david.kennedy@acm.org>

Tue, 26 Dec 2000 13:50:33 -0500

RAF to abandon faulty landing system, by Mark Henderson, science correspondent  
excerpted from <http://www.thetimes.co.uk/article/0,,2-58265,00.html>

ROYAL AIR FORCE pilots will stop using a bad-weather navigation system from January 1 because new commercial radio frequencies have made it unreliable, the Ministry of Defence said yesterday. Pilots of military planes and helicopters fitted with the Instrument Landing System (ILS) will not be allowed to use it to land in poor weather in the new year. Instead they will have to ask air traffic controllers to talk down their flights.

- o Commercial FM growth cited as cause.
- o Commercial ILS on different frequencies has not been affected.
- o Affected aircraft are Nimrod reconnaissance and search and rescue helicopters. RAF transport a/c have already been upgraded and tactical aircraft do not use ILS.

"There is no operational impact whatsoever," a ministry of

Defense

spokeswoman said. "It is a worldwide problem which affects all countries."

"New landing assistance systems use more reliable technology, such as

global positioning satellites, which are not affected by radio frequencies. ILS can also be disrupted by signals from mobile telephones."

Dave Kennedy CISSP Director of Research Services TruSecure Corp.

<http://www.trusecure.com>

---

## ✦ Risks of automatic firmware upgrades

Marc Roessler <marc@tentacle.franken.de>

*Fri, 22 Dec 2000 18:11:30 +0100*

In 1992 ([RISKS-14.06](#)), David Honig reported that a "certain very-popular-workstation-tape-storage-device will reload its firmware upon finding a firmware-reconfiguration tape within its maw upon power-cycling."

Funny how history keeps repeating.. seems the same technique is now used for upgrading the firmware of dolby digital sound processors. Those are used in movie theaters for processing the stream of digital data which is read optically from the 35mm film.

Citing <http://www.dolby.com/cinema/cp500bro.html>:

[..] Moreover, updates to the audio coding used for Dolby Digital soundtracks, which are included from time to time right on Dolby Digital

release prints, download automatically into the CP500 the first time such

a print is played in the cinema. [...]

In a German discussion forum dedicated to the projection of cinema movies

(<http://www.filmvorfuehrer.de/forum/>) on 9 Nov 2000, the

following was

posted by Stefan Mueller:

(translated from German)

The trailer of "Billy Elliott" has got some nasty bug: If the trailer is

being cut right behind start mark three, the CP500 will do a software

reset with data upload as the trailer runs through the machine. Either

Dolby Digital crashes completely or the Cat 673 is set to factory default,

which means setting the digital soundhead delay to 500 perforations,

i.e. the digital sound lags 5.5 seconds behind the picture.

[...]

Nice, isn't it?

Concerning David Honig's report: I own a streamer which seems to have been

built in 1995 (same company? maybe same streamer?), and

according to the

manual it has this "feature", too. Though no power-cycling is necessary, the

firmware upgrade will happen right after inserting the "Firmware Upgrade

Tape" into the drive. I guess this barrier (the need to power-cycle the

device) was removed for better user friendliness.. (or it is some different

kind of streamer and it never had this barrier, which is just as bad). I

won't go into the evil details of what to do to a streamer's firmware in

order to maximize the devastating effect as i am sure you all  
can make up  
some nice ideas yourself.

It seems this "auto-firmware-upgrade" feature is making its way  
in more  
and more products. I just can't wait for cars to be firmware  
upgraded by  
refueling them at the gas station. \*irony\*

---

## **IBM and Intel push copy protection into ordinary disk drives**

John Gilmore <gnu@toad.com>

*Thu, 21 Dec 2000 13:16:03 -0800*

[From cryptography@c2.net; Source:  
Stealth plan puts copy protection into every hard drive  
<http://www.theregister.co.uk/content/2/15620.html>]

\*The Register\* has broken a story of the latest tragedy of  
copyright mania  
in the computer industry. Intel and IBM have invented and are  
pushing a  
change to the standard spec for PC hard drives that would make  
each one  
enforce "copy protection" on the data stored on the hard drive.  
You  
wouldn't be able to copy data from your own hard drive to  
another drive, or  
back it up, without permission from some third party. Every  
drive would  
have a unique ID and unique keys, and would encrypt the data it  
stores --  
not to protect YOU, the drive's owner, but to protect unnamed  
third parties  
AGAINST you.

The same guy who leads the DVD Copy Control Association is

heading the organization that licenses this new technology -- John Hoy. He's a front-man for the movie and record companies, and a leading figure in the California DVD lawsuit. These people are lunatics, who would destroy the future of free expression and technological development, so they could sit in easy chairs at the top of the smoking ruins and light their cigars off 'em.

The folks at Intel and IBM who are letting themselves be led by the nose are even crazier. They've piled fortunes on fortunes by building machines that are better and better at copying and communicating WHATEVER collections of raw bits their customers desire to copy. Now for some completely unfathomable reason, they're actively destroying that working business model. Instead they're building in circuitry that gives third parties enforceable veto power over which bits their customers can send where.

(This disk drive stuff is just the tip of the iceberg; they're doing the same thing with LCD monitors, flash memory, digital cable interfaces, BIOSes, and the OS. Next week we'll probably hear of some new industry-wide copy protection spec, perhaps for network interface cards or DRAMs.) I don't know whether the movie moguls are holding compromising photos of Intel and IBM executives over their heads, or whether they have simply lost their minds. The only way they can succeed in imposing this on the buyers in the computer market is if those buyers have no honest vendors to turn to. Or if those buyers honestly don't know what they are being sold.

So spread the word. No copy protection should exist ANYWHERE in generic computer hardware! It's up to the BUYER to determine what to use their product for. It's not up to the vendors of generic hardware, and certainly not up to a record company that's shadily influencing those vendors in back-room meetings. Demand a policy declaration from your vendor that they will build only open hardware, not covertly controlled hardware. Use your purchasing dollars to enforce that policy.

Our business should go to the honest vendors, who'll sell you a drive and an OS and a motherboard and a CPU and a monitor that YOU, the buyer, can determine what is a valid use of. Don't send your money to Intel or IBM or Sony. Give your money to the vendors who'll sell you a product that YOU control.

John

---

## **✶ CERT's ActiveX security report**

"Richard M. Smith" <rms@privacyfoundation.org>

*Fri, 22 Dec 2000 13:25:20 -0500*

This past summer, CERT sponsored a two-day workshop on security issues with ActiveX controls. The final report was just released today and is available as a PDF file at the CERT Web site:

[http://www.cert.org/reports/activex\\_report.pdf](http://www.cert.org/reports/activex_report.pdf)

There is a lot of good information in the report about how individuals and organizations can reduce security risks in Internet Explorer when using ActiveX controls.

In addition, there is a section aimed at software developers on how to create safer controls.

A good bit of the technical information in the report has not been made public before.

Richard

---

## **✶ Privacy/quality risks in Quicken Online Billing**

"Clay Jackson" <clayj@nwlinc.com>

*Fri, 22 Dec 2000 16:34:34 -0800*

I'm a pretty trusting fellow, and a very early adopter of new technology, but the disclaimer in Quicken 2001's Online Billing agreement gave even me pause:

"...USER ACKNOWLEDGES THAT HE OR SHE BEARS THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE ONLINE BILLING SERVICE"

I'm currently a 'wage slave', but have done my share of consulting - I sure wish I could get this blatant a disclaimer in MY contracts. To add possible injury to the insult, the NEXT page (when I clicked 'Accept' on this) asked me for my SSN, birthdate, place of birth and mother's maiden

name, with NO  
indication as to where and how this information might be used,  
or even if  
the transmission would be 'secure' or encrypted in any way.  
Needless to  
say, I cancelled out of THAT agreement.

Clay Jackson <clayj@nwlink.com>

---

## **✶ Credit report lists ex-spouse's address**

Beth Roberts <eroberts@rult.pair.com>

*Sun, 24 Dec 2000 12:22:18 -0500 (EST)*

Having recently decided to clear up any erroneous black marks on  
my credit  
rating, I ordered reports from both Trans Union and Equifax.  
Both informed  
me that they could not send my credit report because they could  
not verify  
my current address (where I have resided for over a year).

To my surprise, I did receive a copy of my credit report, from a  
company  
called CSC Credit Services. The report gives no clues as to  
whether this  
company is affiliated with Trans Union, Equifax, or neither.

At the top, I see why they had such trouble believing that I  
live where I  
do - all three of the addresses they have listed for me (one  
current, two  
previous) are completely unfamiliar to me. Since they also have  
my name  
listed incorrectly as my married name, I can only assume that  
they had  
surmised I was still living with my ex-husband, and that any  
address

applying to his last name also applied to me.

We have been willfully ignoring each other since the divorce, but it could be dangerous if I were a stalking or vindictive type. This would be an easy way for me to find out where he is, regardless of any measures he might have taken to safeguard his privacy. Alternatively, if I were seeking child support from him, it might come in handy for me. We had no children, so this doesn't apply.

I am not sure whether the same type of mistake is possible in the reverse direction - that is, listing an ex-wife's post-divorce addresses in an ex-husband's credit report. This privacy problem may only occur when there is confusion as to the ex-wife's last name, so it may only potentially reveal the ex-husband.

For me, it's just yet another piece of data I have to get them to correct, in addition to the three (out of ten) incorrect credit history entries that still show a balance due, even though I paid them off.

Beth Roberts <beth@bethroberts.com>

---

## **⚡ Wanna know my salary ?**

John C Haselsberger <jhasels@fast.net>

*Fri, 22 Dec 2000 10:34:33 -0500*

I work for a large corporation that has recently outsourced "employment

verification" (for use in credit applications and such) to a Web-based service, <http://www.theworknumber.com> . This system works as follows: You log into the system with a company code, a Social Security number, and a PIN. You then can generate single-use keys to distribute to those who need your credit or employment verification; then they log onto the same web site with that key and have access to your salary and I believe duration of employment.

To make the system easy-to-use, you can look up a company code given a company name so that this tiny security barrier is useless.

The default PIN is the last 4 digits of your Social Security number. Strike two for Security.

My company has the unfortunate habit of using Social Security numbers, even though each employee has a unique employee number, for identification. Over the years, I have been exposed to many other employees' Social Security numbers, and I can only assume the reverse is true. Strike three.

While we are given the opportunity to change our PIN, the timing of this situation while many people are off on vacation, coupled with human nature, barely lessens this RISK. I called their customer support number, and there is no way to "opt out" of their system.

Whereas they DO use SSL to protect the web transactions, the real risks lie elsewhere.

John Haselsberger <jhasels@fast.net>

---

## ✦ **Re: Spam as a denial of service attack? (Bellovin, [RISKS-21.15](#))**

Steve Wildstrom <steve\_wildstrom@businessweek.com>

*Fri, 22 Dec 2000 10:09:18 -0500*

Interestingly, Verizon has failed to come up, at least in public, with any evidence that this was in fact an attack. Given the company's dubious service record, a lot of folks suspect this may be a pretty lame attempt to blame a popular bogeyman for an inability to handle traffic. Sometimes, I feel that I personally get millions of spam messages a day, but our system generally handles it. An attack would almost certainly have involved a large number of messages from a small number of sources and at least the mail relays that the messages were sent through would have been identifiable, if not the ultimate source.

Steve Wildstrom, Technology & You Editor, \*Business Week\*, 1200 G St. NW #1100  
Washington DC 20005 1-202-383-2203  
steve\_wildstrom@businessweek.com

---

## ✦ **Armageddon scenario near-miss**

Scott Rainey <scott.rainey@webwheels.com>

*Sun, 24 Dec 2000 11:21:46 +0000*

It seems our favorite planet - Earth - barely missed yet another pyrotechnic run-in with a city-killer sized asteroid. It was early Xmas Eve 2000.

Nobody saw it till it had already gone past. Range: 800,000 km. That's barely double the distance of earth to the moon. When you figure that we've got some serious gravity constantly inviting passing space rocks to to pay us a visit, I'd say that it's awful dang close. Although the collision probabilities for us and all known space rocks are officially listed as  $< 1e-9$ , I really don't trust that math.

The risk is in insufficient funding for early warning systems and sub-zero funding for deploying solutions.

If we are REALLY lucky a smallish rock like this one will touch down in a sparsely populated corn field, crating an instant tourist mecca and a kick in the pants for policy wonks.... not to mention a big ratings week for CNN.

news.com.au has the first story of which I am aware @ [http://news.com.au/common/story\\_page/0,4057,1550084%255E1702,00.html](http://news.com.au/common/story_page/0,4057,1550084%255E1702,00.html)

For fresh info on what we claim to know about the sky falling, click to the JPL news page: <http://neo.jpl.nasa.gov/news.html>

[Somewhat off your normal news beat, but I'd bet it is something with high interest for your audience. SR]

[Certainly has risks to computers and related systems, as well as to people. 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 21: Issue 18**

**Thursday 4 January 2001**

## Contents

- [Revenge of Y2K, Norwegian trains halted 31 Dec 2000](#)  
[Jan L](#)
- [7-Eleven unable to process credit cards since 1 Jan 2001](#)  
[Steve Hutto](#)
- [Y2K+1 bug in Sharp Organizer?](#)  
[Philip Berman](#)
- [Power cut hits hundreds of millions in India](#)  
[Edelson Doneel](#)
- [Repeated computer outages for Swedish bank](#)  
[Ulf Lindqvist](#)
- [Telephone outage caused by water-main break](#)  
[Glenn C. Lasher Jr.](#)
- [Computer blamed for Russian rocket crash](#)  
[Peter Neumann](#)
- [Chinook: key facts ignored by those who want to clear pilots](#)  
[John O'Connor](#)
- [CIOs: "What, Me Worry?"](#)  
[NewsScan](#)
- [Automatic firmware upgrades in home electronics](#)  
[Andrew Klossner](#)

- [Hackers hack science exam](#)  
[Winn Schwartau](#)
  - [Re: Seattle Hospital Hacked](#)  
[Daniel Theunissen](#)
  - [Re: IBM and Intel push copy protection ...](#)  
[Patrick P Gelsinger](#)
  - [Re: IMPORTANT MESSAGE FROM EGGHEAD.COM CEO](#)  
[Gary Lawrence Murphy](#)
  - [Re: The risk of a seldom-used URL syntax](#)  
[Crispin Cowan](#)
  - [The top 10 privacy stories of 2000](#)  
[Richard M. Smith](#)
  - [Stefan Brands: PKI, digital certificates, and privacy](#)  
[PGN](#)
  - [Submission Deadline for USENIX Security Symposium, 1 Feb 2001](#)  
[Monica Ortiz](#)
  - [Call For Papers - RAID'2001](#)  
[Giovanni Vigna](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

## ⚡ **Revenge of Y2K, Norwegian trains halted 31 Dec 2000**

<janl@linpro.no>

*Mon, 01 Jan 2001 17:12:21 +0100*

Original story in "Dagbladet ... nettet" in Oslo (In Norwegian:  
<http://www.dagbladet.no/nyheter/2000/12/31/235007.html>)

Abstracted:

In the morning of 31 Dec 2000, departures of the Airport Express train and six "Signatur" departures were hit by a date handling problem. The airport trains were quickly back in action, the 07:28 Signatur departure from

Kristiansand was canceled, and the five other departures were serviced by older trains.

Preben Colstrup, a spokesperson for NSB, verifies that the trains appears to not handle the date 31 Dec 2000 at all, he has no idea why. He promises that all trains will be on schedule on 01 Jan 2001. NSB adds that the trains still have not passed acceptance and belongs to the contractor, Adtranz.

Ronny Solberg in Adtranz says that the problem was solved by setting the date on the trains back a month. It only takes a few minutes, but it took time to get service people around to all the trains. He stresses that all trains were Y2K tested, but that no-one thought of testing 31 Dec 2000. He promises that the problem will be found and fixed permanently.

Dictionary:

- NSB: Norges StatsBaner, the publicly owned train company in Norway
- Signatur and Airport trains: New high speed trains made for NSB by Adtranz. Presumably carrying the same computer systems. Signatur is used for long inter city routes.

Addendum: Later in the day, on national radio news a technical person in NSB speculated that the problem might have been that Y2K was a leap year and the number of days at the end of the year baffled the computers which \*did\* handle 29 Feb 2000 well. There were no reports of non-starters on 01 Jan 2001.

[Quite a few readers noted an AP story in various US sources, including

<http://www.nytimes.com/aponline/technology/AP-Norway-Y2K-Bug.html>

which roughly mirrors the dagbladet item. PGN]

---

## **7-Eleven unable to process credit cards since 1 Jan 2001**

Steve Hutto <shutto@kata.chezns.org>

Wed, 3 Jan 2001 13:43:51 -0700 (MST)

The Denver Post reported today

(<http://www.denverpost.com/business/biz0103e.htm>) that 7-Eleven stores have not been able to process credit-card transactions since January 1, 2001.

The problem appears to be a faulty date-window fix for Y2K, reading the two digit current year of "01" as "1901". A programmatic check in the system rejects credit cards with expiration dates 100+ years in the future. One wonders if they rushed to implement their new information system in order to be Y2K compliant, deciding to skip low-priority system testing to make the deadline. Relevant excerpt from the end of the article:

7-Eleven's retail information system, which handles almost all of the

store's operations, from payroll to purchases, was implemented into all of

its U.S. stores by late 1999. It was deemed Y2K-compliant. The home of

the Big Gulp didn't spend any money to ensure its systems would roll over

correctly from 2000 to 2001. [...]

[Also <http://www.washingtonpost.com/wp-dyn/articles/A16320-2001Jan3.html>]

[More likely a special-case fix that worked \*only\* in 2000, to avoid Y2K, as suggested by Jeremy Epstein. PGN]

---

## 🔥 Y2K+1 bug in Sharp Organizer?

"Berman, Philip" <Philip.Berman@itt.com>

*Wed, 3 Jan 2001 11:30:08 -0500*

I turned my Sharp YO-550 Electronic Organizer on today for the first time since last year. It displayed an error message that all data was corrupted and will be erased. About 4 years of notes and phone numbers lost (yes you can back it up to a computer - The backup kit cost about the same as the organizer). After my initial reaction I turned the unit off and on and it came up seemingly working correctly although it thought it was 1997. I reloaded the current time and date. Upon turning the unit off and on the same error condition resulted (Lost all data including current time and date). Several times I set the date to 2001 with the same error resulting. I then (for some strange reason) tried setting the date to 1/1/2000. The unit worked correctly. In fact with several dates prior to 2001 the error condition never occurred. If I set the date to 2001 or greater it goes into error and loses all memory.

I write to RISKS to find out if other owners of Sharp Organizers have experienced this problem. I have been unable to reach anyone at Sharp (Customer Service Phone is always busy) to comment on the problem.

Philip Berman <philip.berman@itt.com>

---

## **⚡ Power cut hits hundreds of millions in India**

"Edelson, Doneel" <doneel.edelson@eulergroup.com>

*Tue, 2 Jan 2001 12:06:09 -0500*

On 2 Jan 2001, the electrical grid for the entire northern region of India collapsed, affecting 226 million people. The outage began at a substation in Uttar Pradesh, and spread to neighboring states (Punjab, Kashmir, Rajasthan, Haryana and Himachal Pradesh) and to the capital, New Delhi.

Trains, signalling systems, and the New Delhi airport were affected. Demand is often greater than supply, but such widespread outages are apparently

unusual. [PGN-ed; see also

<http://www.cnn.com/2001/ASIANOW/south/01/02/india.blackout/index.html>]

---

## **⚡ Repeated computer outages for Swedish bank**

Ulf Lindqvist <ulf@csl.sri.com>

*Thu, 4 Jan 2001 15:46:33 -0800 (PST)*

As reported in various Swedish news media, The Swedish bank Nordbanken has suffered repeated computer outages during late December and early January. The outages, each with a duration of several hours, shut down ATMs, Internet bank services, debit card purchases and office teller services for Nordbanken's 3.5 million customers.

In an article on the Swedish CNN Web site (cnn.passagen.se) 4 Jan 2001, Nordbanken CEO Magnus Falk says that the bank still does not know what caused the outages, but that they are now able to restart their system faster the next time it crashes...

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/>

---

## **⚡ Telephone outage caused by water-main break**

"Glenn C. Lasher Jr." <glasher@nycap.rr.com>  
*Thu, 28 Dec 2000 16:29:08 -0500 (EST)*

On Thursday, 28 November 2000, 17 of the 21 telephone exchanges in the City of Schenectady NY were taken out of service by a water-main break (for those not familiar with the North American phone system, exchanges uniformly contain a range of 10,000 phone numbers). The Central Office serving downtown Schenectady is located on the block between Franklin and State

Streets and Jay and Clinton Streets. The water main break was on Clinton St, and caused the closure of Clinton and State Streets. The break occurred at 3 AM, and the phones went out around 9 AM.

The cellular telephone networks appear to be unable to cope with the additional traffic. I received a frantic call from my wife, who called me at work from her cell phone to tell me the house phone was out. The signal quality was extraordinarily bad, as is the nature of CDMA digital when the cell is overloaded. One is left to assume that users of FDMA and TDMA-based phones may have been cut off completely, especially analog phone users, where the cells have a hard limit of 20 simultaneous calls.

Meanwhile, my Internet service, provided by TV cable, continues unabated.

So, where do we begin on this one? Well, here are the RISKS:

1. Placement of mission-critical equipment below ground level leaves it susceptible to flooding. One might assume that an unusually heavy downpour might also have caused problems here.

2. This is a good example of network stress, looking at the behaviour of the cellular networks.

3. This is also a classic demonstration of a single point of failure. A problem in one location has cut off a critical service to an entire (although small) city. It does not matter if your service is through the IBOC (Verizon, in this area) or a CLEC (Sprint, AT&T, Met Tel, to name a few), all fo the equipment is owned and maintained by the IBOC

and housed  
at the corner of Franklin and Clinton.

4. It is also a classic demonstration of diverse paths, as my Internet service continues to run. It does not pass through that same building, but is rather located a mile away on Eastern Parkway (or at least I believe that is the location).

glasher@nycap.rr.com

[As an addendum on 29 Dec 2000, the majority of the phone service in the city was restored as of this morning, 29 Dec. During the outage, the city was being patrolled by police, DPW trucks, Amateur (HAM) radio operators, GMRS radio operators, and telco vehicles. A command post was set up at the city police station to serve as a center of all of these diverse communications.

It is further worth noting that the telco vehicles were equipped only with cellular phones for communications. As mentioned before, the cellular networks were next to useless due to traffic overload. For this reason, the ad-hoc radio network that was established became the primary means of emergency communication. This information was gathered by listening on two of the frequencies used: 147.06 MHz (the local HAM repeater) and 462.550 (the GMRS channel that was in local use). Other frequencies could have been monitored as well, but since my monitoring was being sent back out through an MP3 broadcaster, the content needed to be constrained. GCL]

---

## ✂ Computer blamed for Russian rocket crash

Peter Neumann <Neumann@CSL.sri.com>

Mon, 1 Jan 2001 11:01:13 -0800 (PST)

The Ukrainian space rocket design bureau blamed "computer faults" for the failure of a Ukrainian Tsiklon-3 light booster rocket that carried 6 small satellites for the Russian Defense Ministry and space agency Rosaviakosmos.

The rocket engines were shut down 367 seconds after lift-off (presumably

automatically). [Source: CNN, 1 Jan 2001 (a.k.a. as 1/1/01!!!!); PGN-ed;

<http://www.cnn.com/2001/TECH/space/01/01/space.russia.crash.reut/index.html>]

---

## ✂ Chinook: key facts ignored by those who want to clear pilots

"John O'Connor" <jpoc@hotmail.com>

Wed, 03 Jan 2001 18:12:17

The risk of allowing techno mumbo jumbo to get in the way of the truth:

Whenever I read about the Chinook crash on the Mull of Kintyre, I observe that a number of important facts are conveniently ignored. These particular facts are not in dispute and they give incontrovertible proof that the pilots were acting negligently.

Instead, the spectre of some mysterious fault is raised as an argument that the pilots should be absolved of blame.

A few minutes before the accident, the helicopter was traveling at low level across the open sea. It was flying under Visual Flight Rules. VFR involves looking out of the window to see where you are going, which way up you are and to make sure that you do not hit anything. To operate under VFR, requires good visibility. (The actual requirements in terms of how many miles you must be able to see and how far you must be from cloud varies with aircraft type, pilot qualifications and where you are flying.)

The Mull itself was covered in fog and low cloud and, as the flight neared the Mull, it entered this area of reduced visibility. Now, at this point, the crew were in full command of their aircraft and had no technical problems. There has been no dispute over this.

As soon as they encountered the cloud, the crew must have switched to Instrument Flight Rules. That means referring to instruments to see which way is up and to find out where you are and it also means operating at or above the Minimum Safety Altitude. The MSA is defined as being one thousand five hundred feet above the highest obstacle on your flight path or within ten miles either side.

The purpose of these figures is, in part, to give a margin for error but also to give pilots enough room to get out of trouble. For example, an

aircraft flying inside cloud might suddenly find that it is picking up ice sufficient to mean that it cannot maintain altitude. By operating at the MSA, the pilot will have enough room to either side to turn back and fly out of the icing zone and shed the ice before being forced to the ground.

Now, when the pilots of the accident aircraft encountered the cloud and fog around the Mull, they were not only below the MSA, they were actually below the high ground which they were approaching. Given this, the crew were required to make a 180 degree turn and fly out of the cloud. That is what they were trained to do. That is what the law required them to do and that is what the RAF rules required them to do.

Instead, they opted to fly on towards the high ground and attempt to climb over it. Doing so was inarguably an act of negligence or recklessness that endangered the aircraft.

The case that is made, that the aircraft may have suffered from some form of systems glitch that made it incapable of out climbing the rising ground, has no bearing on this. If the pilots had not made the decision to fly, in cloud, towards high ground at an altitude lower than the tops of the hills, the accident would not have happened. The decision that they made went against both their training and the law.

Suppose that I decided to try to drive through the centre of my town as fast as I could and that I found that my brakes failed and I crashed and caused

many deaths. Can I say that it was not my fault and that the accident would have not happened if my brakes had not failed? Of course not. Whether or not there is a problem with the Chinook is an important matter but it does not absolve the crew of the helicopter from blame for entering cloud at such a low altitude. Had they not decided to do that, the accident would not have happened.

John O'Connor: <http://www.jpoc.net>

[In some cases, but not this case, one could ask for a Mull-again (mulligan, or do-over, in golf parlance). PGN]

---

## ✂ CIOs: "What, Me Worry?"

"NewsScan" <newsscan@newsscan.com>

*Thu, 04 Jan 2001 11:53:18 -0700*

A national poll of 1,400 CIOs reveals that 90% have confidence in their network security, despite estimates that billions of dollars are lost every year to cybercrime. The survey, conducted by RHI Consulting, has raised eyebrows among security experts who point out that it's generally in a CIO's best interest to keep quiet when security breaches occur. A recent survey conducted by the Computer Security Institute indicated that more than half of the respondents said they did not report the intrusions to law enforcement out of fear of negative publicity or that rival companies would

use the information to competitive advantage. In addition, many CIOs may feel that they must live with a "buffer of acceptable risk." "Just as credit card companies accept some level of loss as a cost of doing business, so some CIOs are saying, 'if I do a really solid job of protecting my systems, then I can live with the low-level pain that some break-ins cause,'" says one expert. Meanwhile, a 1999 survey found that Fortune 1000 companies lost more than \$45 billion in thefts of proprietary information that year. [\*InfoWorld\*, 3 Jan 2001; NewsScan Daily, 4 Jan 2001]

---

## **⚡ Automatic firmware upgrades in home electronics**

Andrew Klossner <andrew@cesa.opbu.xerox.com>

*Wed, 27 Dec 2000 09:42:45 -0800*

Consumer DVD (video) players are also adopting this "load firmware from a data source" approach. My Phillips-Magnavox DVD850 will slurp up a new firmware load from a DVD. Video DVDs include a good deal of active content, and the industry seems to expand the programming environment on a regular basis. The DVD of the popular movie "The Matrix" wouldn't work at all on half of the installed players when it shipped in 1999 because it used up-to-the-minute constructs.

When the authoritarian software forbids me to skip past a twenty-second copyright notice, it makes me nostalgic for the old 12-inch laser disks.

Andrew Klossner (andrew@cesa.opbu.xerox.com)

## ⚡ Hackers hack science exam

Winn Schwartau <winns@gte.net>

*Thu, 21 Dec 2000 10:36:20 -0500*

Two 8th-grade honor students in Tampa, Hillsborough County, Florida, hacked into the school computer and copied the final exam for one of their courses.

They have been suspended. [PGN-ed]

We've wired up the country's schools, put the kids on the Internet, and only a small handful of teachers have any clue as to what goes on behind the mouse button. The teachers are not technically trained, they are underpaid and underappreciated. Is it any wonder? And I doubt the kids have been taught the first thing about CyberEthics by their schools or their parents.

Winn Schwartau

---

## ⚡ Re: Seattle Hospital Hacked ([RISKS-21.14](#))

"Daniel Theunissen" <dtheunis@earthlink.net>

*Thu, 28 Dec 2000 19:05:17 -0500*

The first response to intrusion news stories by most organizations is almost formulaic: deny the attack, make (often false) allegations that this could

never happen HERE, attack the credibility of the source of the news, and  
lastly take a stand against such heinous activity. The response by the UWMC  
to the intrusion into their network generally follows the formula.

They started back-pedaling the next day:

"We have received the first tangible evidence from news-gathering organizations that someone did, in fact, gain criminal access to a limited  
number of administrative databases that contain some confidential information on at least 5,000 cardiology and rehabilitation  
medicine patients treated at our hospital," said Tom Martin, director and chief  
information officer for University of Washington Medical Centers Information  
Systems.

>From MSNBC: "Hospital Confirms Hacking Incident" 2000-12-8

For more complete coverage, I recommend going to where the story broke:

[www.SecurityFocus.com](http://www.SecurityFocus.com) and search on "University of Washington Medical  
Center"

The original UWMC announcement, however, is still true. Read it carefully,  
they worded it so that they never actually denied the attack.

Dan Theunissen, [dan.theunissen.no.spam@ieee.org](mailto:dan.theunissen.no.spam@ieee.org)

---

**✶ Re: IBM and Intel push copy protection ... (Gilmore, [RISKS-21.17](#))**

"Gelsinger, Patrick P" <[patrick.p.gelsinger@intel.com](mailto:patrick.p.gelsinger@intel.com)>  
*Tue, 26 Dec 2000 06:35:10 -0500*

[Received via Dave Farber, whom Patrick had requested to post a correction.]

Content protection technology misinformation generates negative web-press coverage:

An article on \*The Register\* website "Stealth plan puts copy protection into every hard drive" contains false information that the 4C's (Intel, IBM, MEI, Toshiba) Content Protection for Recordable Media (CPRM) is to be applied to all PC hard drives. It is misinterpreting a specification for use of CPRM with the Compact Flash media format (which supports either semiconductor flash memory or IBM microdrives) probably because Compact Flash uses the same command protocol interface as standard PC harddrives. The technology is neither intended nor licensed for use with PC harddrives and is optional even for the supported media types (flash memory and microdrives). John Gilmore, a noted privacy and consumer advocate, has picked up the article and further propagated the erroneous information and mentioned Intel "IBM&Intel push copy protection into ordinary disk drives". I have alerted public relations at Intel and are disseminating accurate information within Intel and among our industry contacts.

Pat

---

**⚡ Re: IMPORTANT MESSAGE FROM EGGHEAD.COM CEO**

## **(RISKS-21.16)**

Gary Lawrence Murphy <garym@canada.com>

29 Dec 2000 10:23:55 -0500

There is another implicit risk in these stories which I am always quick to bring to the attention of my would-be B2C e-commerce clients.

Suppose you have 500,000 VISA/MC numbers in your computer, and suppose

you have strong cryptographic SSL connections and all that certificate

jazz to ensure the customer and the e-store are who they say they are.

Let's also say that I am an organized crime boss who knows you have

those charge card numbers and have the means and desire to rack up just

\$20 worth of purchase from each of them for a cool fast million dollar

profit ... now (and here's the kicker) what is to stop me from offering

your system administrator some tidy sum (even 10%!) to just slip in

a floppy disk and grab me a copy of the data?

Related to this, I asked a leading e-commerce Web site architect if the DLL

that contained the personal information access username and password might

be used by any program that ran on the server (in java, a class can be

made accessible only to a restricted set of applications). The answer was

that they hadn't thought of that.

Gary Lawrence Murphy <garym@teledyn.com> TeleDynamics

Communications Inc

Business Innovations Through Open Source Systems: <http://www.teledyn.com>

[Simson Garfinkel commented:

I simply do not understand why companies insist on keeping the old VISA/MC numbers in their computers.]

---

## ⚡ Re: The risk of a seldom-used URL syntax (Warnock, [RISKS-21.16](#))

Crispin Cowan <crispin@wirex.com>

Wed, 27 Dec 2000 12:02:24 -0800

This is not new. Spammers have been using these tactics (both @ in the domain name, and decimal and octal IP numbers in place of DNS names) to obscure the actual site hosting their spam content for at least a year. It's annoying, because it takes extra effort to parse out the true host of the web site being spammed. Conversely, its convenient, because it provides incontrovertable evidence that the post in question is a spam, because there is no valid reason to obscure an URL in this way other than to hide the guilty.

Crispin Cowan, Ph.D., Chief Research Scientist, WireX Communications, Inc.

<http://wirex.com> Free Hardened Linux Distribution: <http://immunix.org>

---

## ⚡ The top 10 privacy stories of 2000

"Richard M. Smith" <rms@privacyfoundation.org>

*Thu, 28 Dec 2000 18:24:42 -0500*

It's the end of the year and time for everyone's top 10 list. The Privacy Foundation just released today its top ten list of privacy stories for the year 2000.

Our press release is online at:

<http://www.privacyfoundation.org/release/top10.html>

Richard

---

## **★ Stefan Brands: PKI, digital certificates, and privacy**

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

*Fri, 15 Dec 2000 08:16:00 -0800*

Rethinking Public Key Infrastructures and Digital Certificates:  
Building in Privacy

Stefan A. Brands

ISBN 0-262-02491-8

For more information, please visit

<http://mitpress.mit.edu/promotions/books/BRAUHF00>

[from which this is taken. PGN]

As paper-based communication and transaction mechanisms are replaced by automated ones, traditional forms of security such as photographs and handwritten signatures are becoming outdated. Most security experts believe that digital certificates offer the best technology for safeguarding electronic communications. They are already widely used for authenticating

and encrypting e-mail and software, and eventually will be built into any device or piece of software that must be able to communicate securely.

There is a serious problem, however, with this unavoidable trend: unless drastic measures are taken, everyone will be forced to communicate via what will be the most pervasive electronic surveillance tool ever built. There will also be abundant opportunity for misuse of digital certificates by hackers, unscrupulous employees, government agencies, financial institutions, insurance companies, and so on.

In this book Stefan Brands proposes cryptographic building blocks for the design of digital certificates that preserve privacy without sacrificing security. Such certificates function in much the same way as cinema tickets or subway tokens: anyone can establish their validity and the data they specify, but no more than that. Furthermore, different actions by the same person cannot be linked. Certificate holders have control over what information is disclosed, and to whom. Subsets of the proposed cryptographic building blocks can be used in combination, allowing a cookbook approach to the design of public key infrastructures. Potential applications include electronic cash, electronic postage, digital rights management, pseudonyms for online chat rooms, health care information storage, electronic voting, and even electronic gambling.

Stefan A. Brands is Distinguished Scientist at Zero-Knowledge Systems, Inc., Montreal, Canada.

## **✦ Submission Deadline for USENIX Security Symposium, 1 Feb 2001**

Monica Ortiz <monica@usenix.org>

*Thu, 04 Jan 2001 13:31:07 -0800*

10th USENIX Security Symposium 2001 Conference

13-17 August 2001, Washington, D.C., USA

Conference URL: <http://www.usenix.org/events/sec2001>

Sponsored by USENIX, the Advanced Computing Systems Association

Paper submissions due: 1 February 2001

Program Chair Dan S. Wallach, Rice University

Invited Talks Coordinator Greg Rose, Qualcomm

For more details on the submission process, authors are encouraged to consult the detailed author guidelines on the symposium website at:

<http://www.usenix.org/events/sec01/cfp/guidelines.html>

USENIX Security Symposium 2000 is sponsored by USENIX, the Advanced Computing Systems Association, USENIX is an international membership society.

---

## **✦ Call For Papers - RAID'2001**

Giovanni Vigna <vigna@cs.ucsb.edu>

*Tue, 02 Jan 2001 07:03:57 -0800*

Fourth International Symposium on Recent Advances in Intrusion Detection

10-12 October 2001, University of California, Davis, CA, USA

[Abridged for RISKS. See <http://www.raid-symposium.org/Raid2001> for

complete notice -- and by 31 Jul 2001, the preliminary program. PGN]

RAID executive committee chair: Marc Dacier (IBM Research, Switzerland)

Program co-chair: Wenke Lee (NC State University, USA)

Program co-chair: Ludovic Me (Supelec, France)

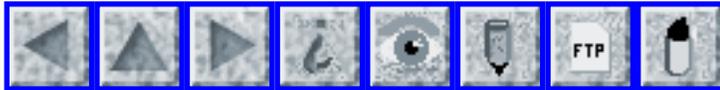
Full and short papers submitted [by 30 Mar 2001] to RAID must be original

contributions, not published or submitted to other conferences.

Full papers

are limited to 6000 words, short papers to 2000, full page figures being

counted as 300 words. [...]



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 21: Issue 19**

**Tuesday 9 January 2001**

## Contents

- [Security at UK nuclear power stations](#)  
[Brian Randell](#)
- [Re: Revenge of Y2K, Norwegian trains halted 31 Dec 2000](#)  
[Bob Dubery](#)
- [Motorola flex non-non-non-leap year](#)  
[Dan Jacobson](#)
- [Millennium error in Postscript calendar](#)  
[Eric Lindsay](#)
- [Two satellite failures](#)  
[Peter B. Ladkin](#)
- [Teen intercepts MD's pages, makes medical orders](#)  
[Terry Carroll](#)
- [Dutch Railways to introduce electronic access/ID card](#)  
[Marcus de Geus](#)
- [Risks of "upgrades" and network-centric applications](#)  
[Jay R. Ashworth](#)
- [Re: Chinook](#)  
[Phil Payne](#)  
[Ryan O'Connell](#)
- [Re: CIOs: "What, Me Worry?"](#)

[Mark Hull-Richter](#)

- [Re: Egghead.com](#)  
[Jonathan Kamens](#)  
[Mark Hull-Richter](#)
  - [Re: Y2K+1 bug in Sharp Organizer](#)  
[Philip Berman](#)  
[Jonathan Kamens](#)
  - [Re: IBM and Intel push copy protection](#)  
[David Collier-Brown](#)
  - [Security white paper](#)  
[Gene Spafford](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

## ✶ Security at UK nuclear power stations

Brian Randell <Brian.Randell@newcastle.ac.uk>

*Tue, 9 Jan 2001 10:16:27 +0000*

There is an article in today's Guardian starting:

"Tough new security checks are to be imposed at nuclear power stations

after a guard employed to protect the station attempted to sabotage the

site's computers . . ."

Apparently he was caught hacking the power station's system in June

1999 "to alter sensitive information".

The full text is at

<http://www.guardianunlimited.co.uk/nuclear>

Brian Randell

Dept. of Computing Science, University of Newcastle, Newcastle

upon Tyne,  
NE1 7RU, UK Brian.Randell@newcastle.ac.uk +44 191 222 7923

[Seen by Dave Stringer-Calvert at

[http://news.bbc.co.uk/hi/english/uk/newsid\\_1107000/1107353.stm](http://news.bbc.co.uk/hi/english/uk/newsid_1107000/1107353.stm)

-- which notes that the guard had never been vetted and had two undisclosed criminal convictions. The Bradwell magnox reactor in Essex

is the nearest nuclear power generator to London. PGN]

---

## **★ Re: Revenge of Y2K, Norwegian trains halted 31 Dec 2000** **(RISKS-21.18)**

"Bob Dubery" <bdubery@netcare.co.za>

*Fri, 5 Jan 2001 09:13:12 +0200*

One possible cause of the inability to handle 31 Dec 2000 is a potential bug

that year2000.com warned about some time ago:

<http://www.year2000.com/y2kcurrent1.html>

Usually a year spans 53 calendar weeks or part weeks. But 2000 spanned 54

weeks or part weeks. This occurs every 28 years. In 1972, computer systems

and embedded code were not as pervasive as they are now.

If a system has software that uses the number of the calendar week, then it

may have problems on 31 Dec 2000 which is the start day (and only day) of week 54.

[The year 2000 began on a Saturday and ended on a Sunday; ergo, 54

calendar weeks. PGN]

## ✶ Motorola flex non-non-non-leap year

Dan Jacobson <jidanni@kimo.FiXcomTHiS.tw>

07 Jan 2001 06:26:43 +0800

My Motorola flex page knows about leap years, and that every 100 years is a non leap year, and every 400 years is a non-non-leap year, but it didn't know every 1000 years is a non-non-non-leap year, well, something like that, anyways, had to set it to 1996 at the millennium.

<http://www.geocities.com/jidanni> Tel886-4-25854780 e-mail: restore .com. ¿nα|¥\$

---

## ✶ Millennium error in Postscript calendar

Eric Lindsay <eric@wrevenge.com.au>

Sat, 06 Jan 2001 20:26:22 GMT

For the decade and more I have been printing myself a monthly calendar using a free Postscript program.

```
%!  
% PostScript program to draw calendar  
% Copyright (C) 1987 by Pipeline Associates, Inc.  
% Permission is granted to modify and distribute this free of  
charge.
```

I checked for Y2K errors, and had no problem with the output. However it turned out the first calendar for 2001 was in error by several days.

```

/startday {
    % starting day-of-week for this month
    /off year 3000 sub def % offset from start of "epoch"
    off
    off 4 idiv add % number of leap years
    off 100 idiv sub % number of centuries
    off 1000 idiv add % number of millennia
    1 add 7 mod 7 add % offset from Jan 1 3000
    /off exch def
    1 1 month 1 sub {
        1 copy
        days_month exch 1 sub get
        exch 2 eq
        isleap and
        {
            1 add
        } if
        /off exch off add def
    } for
    off 7 mod % 0--Sunday, 1--monday, etc.
} def

```

The code was originally starting from 2000. As you can see, you can be pretty arbitrary about starting dates.

However, I wonder how many other calendar programs out there are also working their way backwards from some fairly arbitrary date, rather than forwards from some date in the past?

Eric Lindsay <http://psiphi.server101.com/airlie>

Airlie Beach Qld Australia - Great Barrier Reef entry

---

## ✶ Two satellite failures

"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>

*Sun, 07 Jan 2001 18:37:55 +0100*

"The Boeing Satellite Systems (formerly Hughes Space and

Communications)-

built Galaxy VII communications satellite operated by PanAmSat has stopped functioning in geostationary orbit following a spacecraft control processor (SCP) fault that has hit several sister satellites." (Flight International, 5-11 December 2000, p34, article "Control fault knocks out Galaxy" by Tim Furniss. The capitalised "G" is important.)

This wasn't the first. The craft lost its first SCP in June 1998. The second SCP stopped functioning on 25 November 2000; the craft lost attitude control and its solar panels lost track of the sun.

Apparently, tiny crystalline structures can grow and bridge the terminals of tin-plated relay latching switches to their case, causing a short circuit. People have known about it since a Hughes analysis in 1995 from telemetry data, but there isn't much one can do about it on satellites launched years before. "It is believed" that the builder switched to nickel plating from tin in 1997.

The EarthWatch Quick Bird 1 satellite may have suffered from a computer error, causing its solar arrays to deploy while still attached to the ascending Cosmos 3M booster rocket, launched from Plesetsk on 21 November 2000, according to a report in Flight International (12-18 December 2000, p36) citing "Russian officials". The satellite was lost, which resulted in "48 employees or 24% of the work force of EarthWatch being laid off".

Peter Ladkin

## 🔥 Teen intercepts MD's pages, makes medical orders

Terry Carroll <carroll@tjc.com>

Mon, 8 Jan 2001 16:13:13 -0800 (PST)

AP reports that a Virginia teenager obtained a pager used by the Inova Fairfax Hospital, in Fairfax Virginia. According to the article, he then "gained access to the hospital's paging system" (the article is not clear on whether this was a hack, or what) and forwarded a physician's number to his pager.

When the physician was paged, the allegedly boy returned the calls and gave the nurses medical orders, including authorizing prescriptions and minor medical procedures (such as blood tests and oxygen administration). According to the Washington Post, he is believed to have issued "about a dozen orders."

Yikes.

<<http://news.findlaw.com/ap/o/1110/1-4-2001/20010104042024690.html>>; also, <<http://www.washingtonpost.com/wp-dyn/articles/A14467-2001Jan3.html>>.

An earlier report by the Post notes that:

The court papers and hospital say that on the overnight shift of Dec.

7-8, the youth ordered 12 treatments for six patients. His orders

allegedly included prescribing the blood thinner heparin and

asking for  
blood tests and oxygen for patients.

In each case, the orders were medically "appropriate under the circumstances," said Russell Seneca, chief of surgery at the hospital.

<<http://www.washingtonpost.com/wp-dyn/articles/A13455-2000Dec15.html>>

Terry Carroll, Santa Clara, CA carroll@tjc.com

---

## **✶ Dutch Railways to introduce electronic access/ID card**

Marcus de Geus <marcus@degeus.com>

*Sun, 31 Dec 2000 13:31:14 GMT*

On 28 Dec 2000, \*De Volkskrant\*, one of the leading Dutch morning papers, reported on its front page that NS, the Dutch Railways, are set to invest 3,000 million guilders (approx. 1,400 million euro) over the next decade "to improve the quality of service". The article reads like a "for your convenience" notice.

One of the main items (at 1,100 million guilders) scheduled for improvement is public safety on platforms. Improved safety is to be achieved through the introduction of CCTV cameras and electronic access barriers. In time (the year 2002 is mentioned), the latter are to restrict platform access to persons carrying (and presumably, swiping) a Public Transport Chipcard, which will also act as a means of identification. The chipcard

scheme alone  
is budgeted at 500 million guilders.

One obvious risk to the public is of course the connection the scheme will provide between two hitherto distinct sets of demographics. The real-time linking of personal data to transport information will no doubt prove to be irresistible to marketers should the scheme ever come to fruition.

Another, perhaps less obvious, risk concerns the loss of quality of service resulting from such a scheme. Will incidental travelers be forced into separate queues to have their photographs taken and their personal details checked? How will incoming cross-border rail passengers be expected to cope? What happens to flight passengers arriving at Schiphol airport, one of the main transit points in the Dutch railway system? The mind boggles.

Marcus de Geus <marcus@degeus.com> <http://www.degeus.com>

---

## **⚡ Risks of "upgrades" and network-centric applications**

"Jay R. Ashworth" <jra@baylink.com>  
*Tue, 9 Jan 2001 15:21:59 -0500*

Regular readers of RISKS will of course be familiar with the syndrome described here, but the lesson bears repeating because, apparently, some people still haven't gotten with the program.

The State of Florida, in the last 3 years or so, has a) turned

over all it's  
tele- and data-communications business to a single vendor (that  
this vendor  
is Intermedia Communications, for whom I have a personal and  
professional  
distaste isn't especially germane to this discussion) and b)  
replaced their  
vehicle registration management computer software system.

(What they replaced it with was one of those horribly  
inefficient "make a  
3270 look like Windows" things that are all the vogue these days  
-- with  
everyone except the poor front-end operators, but *\*that's\** not  
directly  
germane, either. :-{ )

What *\*is\** on point here is that new system (b) doesn't allow off-  
line  
transactions to be made in any fashion except by hand, on legal  
pads, and,  
of course, the network (a) failed yesterday for between 4 hours  
and all day,  
depending on which office you were in, because of "an incomplete  
overnight  
attempt to upgrade the fiber-optic communications network",  
according to a  
story in today's St Petersburg Times, at  
[http://www.sptimes.com/News/010901/TampaBay/  
Technical\\_glitch\\_stal.shtml](http://www.sptimes.com/News/010901/TampaBay/Technical_glitch_stal.shtml)

No matter *\*who\** the carrier is, if you've only got one, you'd  
better have  
your backup plans in order. If you've only got one carrier, and  
you *\*don't\**  
have a manual fallback option, you'd better have the number for  
Office  
Depot's delivery desk.

Have *\*you\** looked at your "emergency preparedness" binder lately?

Jay R. Ashworth <jra@baylink.com> Baylink The Suncoast Freenet  
Tampa Bay, Florida <http://baylink.pitas.com> +1 727 804 5015

## ✉ **Re: Chinook ([RISKS-21.18](#))**

<phil@isham-research.freemove.com>

Sat, 06 Jan 2001 12:04:39+0000

The debate about the Chinook accident continues and progress is slow. I suggest using <http://www.computerweekly.co.uk> and entering 'CHINOOK' as a search argument.

There are many aspects of RISK. One is undoubtedly that of putting all your eggs in one basket - flying such a concentration of critical expertise in a single aircraft was reckless; the more so because they were engaged in activities so vital to anti-terrorist efforts.

Another is flying a significant number of passengers in an aircraft equipped with neither a flight data recorder nor a cockpit voice recorder. This is the computing-related risk - we simply do not know what actually happened on the flight, except that 29 people died.

The third was previously unknown - that serving officers of the British armed forces could be posthumously condemned for gross negligence, even though the Queen's Regulations under which they operate specifically forbid this in the absence of conclusive proof.

Yes - the apparent actions of the pilots appear to contravene their training

and orders. But we don't know for certain what happened on the flight, and that's the key risk the Royal Air Force ran. Many people (including a substantial number of Members of Parliament) agree that the dead officers' families should not be used as scapegoats for the authorities' use of a single aircraft and their failure to provide data and voice recording on a passenger flight, especially where specific safety concerns existed about both the particular aircraft and the type in general.

Phil Payne <http://www.isham-research.freeseerve.com>

---

## **✶ Re: Chinook ([RISKS-21.18](#))**

"Ryan O'Connell" <[ryan@complicity.co.uk](mailto:ryan@complicity.co.uk)>  
*Fri, 5 Jan 2001 08:30:25 +0000*

The distinction between VFR and IFR is purely a civil aviation one. Military pilots are not constrained in such a way, and have a number of systems at their disposal that civil pilots do not have.

> ... the crew were required to make a 180 degree turn and fly out of the  
> cloud. That is what they were trained to do. That is what the law required  
> them to do and that is what the RAF rules required them to do.

This is what civil flight rules required them to do, not what RAF rules required them to do.

The RAF pilots broke civil flight rules, which they are quite

entitled to do. Military pilots are required to follow civil flight rules only when it does not interfere with operations. Given that the aircraft was carrying a number of prominent anti-terrorist figures and that Northern Ireland is generally regarded as a war zone as far as the military is concerned, the pilots would have been following war-time military rules and not civil flight rules.

RAF jet and helicopter pilots are highly trained in "Nap of Earth" flying, which involves flying as close to the ground as possible even in adverse weather conditions and was used to great effect in the Gulf War. The Chinook would have been fitted with a terrain-following radar for exactly this purpose, which the pilots would have been using. (This is not the same system as Civil radar altimeters, military systems show the pilot the "shape" of the terrain in front of the aircraft)

Flying at 1,500m (about 4000ft) above the high point would expose the aircraft to anti-aircraft fire, and is probably not within the capability of the aircraft in any event. (Chinook aircraft have a service ceiling of about 2500m, and Scotland has quite a number of large hills) It seems in this case that the RISK of flying under civil rules and being shot down was deemed greater than the RISK of flying under military rules - the military are trained to take risks, and if that judgment was incorrect it should be the officers in charge that are responsible, not the pilots.

Ryan O'Connell - <ryan@complicity.co.uk> - <http://www.complicity.co.uk>

---

## ✉ Re: CIOs: "What, Me Worry?" ([RISKS-21.18](#))

Mark Hull-Richter <Mark.Hull-Richter@quest.com>

*Fri, 5 Jan 2001 17:19:19 -0800*

> ... Meanwhile, a 1999 survey found that Fortune 1000 companies  
lost  
> more than \$45 billion in thefts of proprietary information that  
> year. [*\*InfoWorld\**, 3 Jan 2001; *NewsScan Daily*, 4 Jan 2001]

I am HIGHLY skeptical of all claims of losses by large corporations. The Virus Myths web page (<http://www.vmyths.com>) is replete with examples of hyperbole and exaggerated claims of losses due to viruses and virus hoaxes without one shred of substantive evidence to back up those numbers. How does this \$45 billion number come about? How does a company arrive at the amount of money they actually lost due to theft of proprietary information? (How does one quantify such a loss anyway? Was the theft before or after the information gained value by market success of the product? Either way, these numbers are all estimates since they can't be physically quantified unless a lawsuit is involved, in which case the "loss" is recoverable.)

Notice at least that they didn't have the audacity to blame the losses on hacking incidents, just "theft of proprietary information."

## ✶ Re: Egghead.com (Murphy, [RISKS-21.18](#))

Jonathan Kamens <jik@kamens.brookline.ma.us>

Mon, 8 Jan 2001 22:52:03 -0500

Such a scheme would almost certainly be detected quite easily. If only 1% of the 500,000 credit card users check their statements every month and report charges they didn't make (and I imagine that in fact the percentage is higher than that; you do, don't you? I certainly do), the various credit card companies will be hit with 5,000 complaints in short order. Each credit-card company has legions of people and computers looking for patterns to detect cases of extensive fraud. Furthermore, I imagine that the various credit-card companies work together in some way to combat fraud, so their information would be pooled.

Even if the number of customers reporting the bogus charges is low, surely the credit-card companies' fraud prevention algorithms will be suspicious of a new merchant suddenly ringing up tens of thousands of dollars in purchases, at least suspicious enough to flag the merchant's account for a human being to examine more closely? Merchants do *\*not\** get their money from the credit-card companies immediately, you know.

Once the fraud is detected, its pattern is usually easy to determine (the credit-card companies do, after all, have auditable trails of all charges

going back for quite a long time; if the trail isn't auditable, then how does the "organized crime boss" get his money?) and the credit-card companies can recover the money from the company which placed the illegal charges on the cards.

The usual strategy for preventing the bilked customers from complaining is to give the front company a name that makes it look like a pornographic Web site or telephone hotline. This is supposed to make most people too embarrassed to complain about the errant charge. I find it hard to believe that this is particularly effective, considering that we read about these failed schemes over and over in the newspapers.

To pull off this kind of fraud successfully, you need to have control over a large number of mostly legitimate merchants who are willing to launder the bogus charges for you, you need to make the amounts of the bogus charges small, and you need to spread them out over time rather than charging them all at once. All of these restrictions obviously limit the amount of profit you can successfully reap from such a scheme. And even if you are successful for a time, there's always a chance that one of the credit-card companies will catch up with one of the merchants, and there's always a chance that the merchant will sing like a canary when he's supposed to be clamming up about where he got those credit-card numbers from.

>[Simson Garfinkel commented:

> I simply do not understand why companies insist on keeping the old

> VISA/MC numbers in their computers.]

Because what the focus groups tell them, over and over again, is that shopping on-line has to be fast and painless, and the faster and more painless it is, the more likely it is that customers will keep using your site. If two sites are equal in all ways except that one of them stores your credit-card number so you don't have to reenter it and the other one doesn't, the one with the stored numbers has a competitive advantage. People care more about saving thirty seconds every once in a while than they do about the remote chance that their credit-card numbers might be stolen by a hacker.

I can't say that I particularly blame them. How many people, really, are damaged by fraudulent charges on their credit cards which can be traced to numbers stolen from Web sites? How often do such fraudulent charges go uncaught by the credit-card companies?

I confirm every item on every credit-card statement I receive. Anyone who does so has nothing to fear from hackers breaking into Web sites and stealing lists of credit-card numbers. In my opinion, anyone who does *\*not\** do so is being foolish, regardless of whether they allow their credit-card numbers to be stored on Web sites.

Jonathan Kamens

## **✶ Re: Egghead.com (Murphy, [RISKS-21.18](#))**

Mark Hull-Richter <Mark.Hull-Richter@quest.com>

*Fri, 5 Jan 2001 17:19:19 -0800*

> Suppose you have 500,000 VISA/MC numbers in your computer,  
[...]  
> and have the means and desire to rack up just \$20 worth [...] for a  
> cool fast million dollar profit [...] what is to stop me from offering  
> your system administrator some tidy sum (even 10%!) to just slip in  
> a floppy disk and grab me a copy of the data?

Last I checked, \$20 x 500,000 is \$10,000,000 - that 10% just got a LOT bigger...

---

## **✶ Re: Y2K+1 bug in Sharp Organizer ([RISKS-21.18](#))**

"Berman, Philip" <Philip.Berman@itt.com>

*Mon, 8 Jan 2001 07:39:51 -0500*

This is an update of my previous posting. I was able to reach Sharp Customer Service and the problem has been verified by them. It seems to be isolated to only the model YO-550. In addition my report that it seemed to be a 2001 problem is not entirely accurate. The condition (loss of all memory) occurs when the two least significant digits of the date fall between 01 and 49. Thus setting the calculator to 1901 will cause the problem. If I just wait for 2050 the problem will go away.

Not only has Sharp confirmed the problem, but they have indicated that they will exchange my organizer for a new model.

Philip Berman <philip.berman@itt.com>

---

## ✉ **Re: Y2K+1 bug in Sharp Organizer? (Berman, [RISKS 21.18](#))**

Jonathan Kamens <jik@kamens.brookline.ma.us>

*Mon, 8 Jan 2001 22:28:56 -0500*

>About 4 years of notes and phone numbers lost (yes you can back it up  
>to a computer - The backup kit cost about the same as the organizer).

And what is the "cost" of reconstructing the four years of notes and phone numbers? I can't imagine that it's less than it would have cost to buy and use the backup kit.

In my opinion, this point is as important as Mr. Berman's main point about the failure of his Sharp organizer (and presumably many others) when confronted with dates in 2001: If your data is worth keeping, it's probably worth backing up.

According to the Sharp Web site, the cable for connecting Mr. Berman's organizer to a PC costs \$49.99 and the software to use with it costs \$99.99. Admittedly, that's a bit pricey, but is \$150, amortized over four years, really more expensive than the aggravation caused by the loss of

the data?

When my brother gave me an organizer as a gift years ago, the first thing I did was figure out how I could transfer its data to/from my computer. I refused to store *\*any\** data on it until I was confident that I would not lose anything when it died. And indeed, when I finally dropped it one too many times and it gave up the ghost, all of its data was backed up intact on my PC and I didn't lose anything.

Incidentally, the Sharp Electronics Web site (<http://www.sharpelectronics.com/about/AboutY2k/0,1334,,00.html#YO550>)

says that Sharp is aware of this problem and will replace any affected YO-550, free of charge. It also confirms that, "UNFORTUNATELY, ANY CUSTOMER ENTERED DATA FROM THE DEVICE NOT BACKED UP TO A PERSONAL COMPUTER WILL NOT BE RECOVERABLE."

Jonathan Kamens

---

## ⚡ Re: IBM and Intel push copy protection (Gelsinger, [RISKS-21.18](#))

David Collier-Brown <David.Collier-Brown@canada.sun.com>

*Fri, 05 Jan 2001 09:40:09 -0500*

This explanation may be erroneous: a member of the ATA committee is cited at

<http://www.ihateapple.com/> "Hard Drive Copy Protection Update"

as saying

that IBM has in fact proposed a set of ATA commands to do so.

The Register has followed up by posting a set of frequently asked questions, including a counter-argument to the claim that the extension is only for removable media.

Read the article at <http://www.theregister.co.uk/content/2/15718.html>

and make up your own mind.

dave David Collier-Brown, Performance & Engineering Team,  
Americas Customer  
Engineering (905) 415-2849 davecb@canada.sun.com

---

## ✦ Security white paper

Gene Spafford <spaf@cerias.purdue.edu>

*Fri, 29 Dec 2000 20:50:19 -0500*

Risks readers may be interested in the report at this link:

<[http://www.cerias.purdue.edu/events/summit\\_4q2000.php](http://www.cerias.purdue.edu/events/summit_4q2000.php)>

From that page:

Extraordinary changes in the way we do business and lead our lives in the ever-connected world of the future will create tremendous security challenges. These challenges will be shaped by many of today's emerging trends: the rapid acceleration of network speed, connectivity and the overall number of devices; the removal of the human element from many everyday transactions; and easier and cheaper collection of public and private information. More than ever before, we will demand security

solutions that enable businesses to thrive and private information to be protected.

Accenture has just released the Security Call to Action and executive summary, from the 15 security experts who participated in the CERIAS Security Vision Roundtable. This two-day event, jointly sponsored by Accenture and the Purdue University CERIAS (Center for Education and Research in Information Assurance and Security), brought together both industry pioneers as well as information security leaders experts at some of the largest and most influential companies in the world. The report includes a Call to Action and a list of the key trends affecting security over the next decade. The bottom-line is that doing security right requires the greater community of business leaders, technologists, educators and political leaders to look seriously at this Call to Action and to commit resources and energy to help lead us all to a more secure world.

Accenture is the new name for Andersen Consulting as of January 1, 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 21: Issue 20**

**Saturday 13 January 2001**

## Contents

- [Dell, Unisys and Microsoft -- DUMvoting 1.0!](#)  
[Gene N Haldeman](#)
- [San Francisco Airport radar phantom flights](#)  
[PGN](#)
- [Cell phone in luggage alarms avionics](#)  
[David Kennedy](#)
- [Testimony before the U.S. Civil Rights Commission](#)  
[Douglas W. Jones](#)
- [No human finger will actually pull a trigger...](#)  
[Daniel P. B. Smith](#)
- [Swiss debit-card system broke down](#)  
[Andre Oppermann](#)
- [Subject: Re: The Chinook Crash](#)  
[Peter B. Ladkin](#)  
[Mike Beims](#)
- [Armchair Chinook RISKS analysis is misplaced](#)  
[Nathan K. Pemberton](#)
- [Since when is Northern Ireland considered a war zone?](#)  
[Chris Warwick](#)
- [Oregon Jurors summoned for 1901](#)

[Aydin Edguer](#)

● [Y2K bug in Millennium clock](#)

[Mike Palmer](#)

● [Re: 54 weeks in a year?](#)

['o-Dzin Tridral](#)

[Paul van Keep](#)

● [Info on RISKS \(comp.risks\)](#)

---

## ⚡ **Dell, Unisys and Microsoft -- DUMvoting 1.0!**

Gene N Haldeman <gene@gene-haldeman.com>

*Fri, 12 Jan 2001 17:56:28 -0500 (EST)*

[It is never too early for April to roll around. PGN]

"This Message Can Not Be Considered Spam, Even Though It Is.  
Some Law That Never Was Enacted Says So."

Dell, Unisys and Microsoft have joined together to produce:  
DUMvoting 1.0!

DUMvoting 1.0 is a simple 375k zipped download which you can  
install on  
your machine tonight, and vote for President tomorrow! Worried  
about  
hanging chad? Not with DUMvoting 1.0! No, your vote will  
travel over  
HEALTHY SAFE Internet connections to our new DUMvoteCenter,  
located in my  
next-door neighbor's basement where a 16-year-old computer  
genius known as  
SWORDGANDALF will convert it into paper ballots in between  
Dungeons and  
Dragons games.

(Note: During installation, a pop-up box may notify you that  
Back Orifice  
is being installed. This is normal. For best results, please

disable all  
anti-virus software before installing DUMvoting 1.0)

NEVER AGAIN will you walk to a voting booth in the rain. NEVER AGAIN will you have to associate with the kind of people (and you know what I'm talking about, I don't have to spell it out for you, do I?) who hang around the voting area. NO MORE messy contact with neighbors. We have got it ALL WORKED OUT for you.

And with our new SPEEDYEXITPOLL (c), you won't have to wait till midnight for the outcome! We will be sending our projections the day before the elections, and our exit polls by 11:30 am on election day, saving you both time and anxiety.

You must act fast, but DUMvoting 1.0 can be rushed to you for the low, low price of \$299.00 from our website at DUMvoting.com. In addition, we will send you OILMAN 3.2, the exciting new game from Microsoft: Alaska's Up For Grabs, And You Have Just Been Appointed To The EPA! Plunder as you will, but watch out for the charging caribou; we're told they have a "thing" for the pipeline!

Order without delay. Please include your Social Security number and any recent medical bills.

\*Sent by the Dell/Unisys/Microsoft Consortium: "DUMideas Last Forever."

[Note that DUM spelled backwards is MUD. Must be symbolic.  
PGN]

## **✈ San Francisco Airport radar phantom flights**

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

*Tue, 9 Jan 2001 14:48:49 PST*

The effort to install a new ground radar system for collision avoidance has been set back by the appearance of phantom planes. In earlier tests, a Fremont-based component created ghost images for six nonexistent planes, giving the appearance that two planes were heading for the same runway. The bug has finally been identified (according to a radio report), but it must now be fixed, whereupon tests will continue. [Source: Wire services, 8-9 Jan 2000]

---

## **✈ Cell phone in luggage alarms avionics**

David Kennedy CISSP <david.kennedy@acm.org>

*Fri, 12 Jan 2001 02:18:54 -0500*

Reuters noted that a Slovenian Adria Airways airplane made an emergency landing in Ljubljana on 9 Jan 2001 because of a cell phone in the baggage hold had been left on. It is asserted that the ringing phone corrupted plane avionics and triggered a fire indicator. [PGN-ed from <http://www.theregister.co.uk/content/5/15995.html>]

I'm not certain how this should be classified:

Remarkable detection of RFI without instrumentation?  
Remarkable instance of RFI?  
Remarkable instance of attributing flight instrument  
irregularities  
to RFI after an aborted flight?

Rhetorical: If this had occurred in the US, would the incident  
have  
counted against the airline's on-time statistics?

Dave Kennedy CISSP Director of Research Services TruSecure Corp.  
<http://www.trusecure.com>

[Also noted by Aydin Edguer at  
[http://dailynews.yahoo.com/h/nm/20010110/od/aircraft\\_dc\\_1.html](http://dailynews.yahoo.com/h/nm/20010110/od/aircraft_dc_1.html)

PGN

---

## **✶ Testimony before the U.S. Civil Rights Commission**

Douglas W. Jones,201H MLH,3193350740,3193382879 <jones@cs.uiowa.edu>  
*12 Jan 2001 22:46:04 GMT*

My testimony before the United States Civil Rights Commission  
hearing on  
allegations of election-day irregularities in Florida, Jan 11  
2001, is  
indexed on the Web at  
<http://www.cs.uiowa.edu/~jones/voting/usrc.html>

My testimony was presented as part of the Expert Panel on Voting  
Technology,  
along with testimony from Kimball Brace (Election Data Services)  
and John  
Ahmann (Election Supplies Inc, the major Votomatic vendor). My  
testimony  
and Brace's testimony were in strong agreement on key issues  
involving

information that must be reported in the canvass of an election that is very irregularly reported today. I made strong statements about the risks of standardizing election technology, as opposed to setting performance standards, and I pointed out major problems with the current regulation of computer software used in elections.

It was covered live on CSPAN, and if the USCRC follows its usual procedure, multimedia transcripts of the oral testimony (audio and video) will be on their web site in about a month.

Doug Jones <jones@cs.uiowa.edu>

---

## **✶ No human finger will actually pull a trigger...**

"Daniel P. B. Smith" <dpbsmith@world.std.com>

*Fri, 12 Jan 2001 16:10:55 -0500*

"Hemos," in an article in Slashdot, called my attention to <http://www.cnn.com/2001/US/01/12/airborne.laser/index.html> This describes a weapons system under development, in which a Boeing 747 will carry an airborne laser capable of shooting down missiles. According to the article:

No trigger man

No human finger will actually pull a trigger. Onboard computers will decide when to fire the beam.

Machinery will be programmed to fire because human beings may

not be fast

enough to determine whether a situation warrants the laser's use, said

Col. Lynn Wills of U.S. Air Force Air Combat Command, who is to oversee the battle management suite.

The nose-cone turret is still under construction

"This all has to happen much too fast," Wills said. "We will give the

computer its rules of engagement before the mission, and it will have

orders to fire when the conditions call for it."

The laser has about only an 18-second "kill window" in which to lock on

and destroy a rising missile, said Wills.

"We not only have to be fast, we have to be very careful about where we

shoot," said Wills, who noted that the firing system will have a manual

override. "The last thing we want to do is lase an F-22 (fighter jet)."

"I should've done better, didn't mean to be unkind.

Y'know that was the last thing on my mind..."

Daniel P. B. Smith <dpbsmith@world.std.com>

---

## **✶ Swiss debit-card system broke down**

Andre Oppermann <oppermann@telehouse.ch>

*Wed, 10 Jan 2001 01:23:39 +0100*

On the day before Christmas Eve, usually the day with the highest turnover

of the year in all shops, the whole Swiss debit-card (EC-Card)

processing

system of Telekurs broke down for more than two hours. Also

getting Money

from ATM's and the processing of on-line MasterCard credit card payments,

which is handled by the same company, was interrupted.

In Switzerland the debit card "EC card" is quite popular and nearly everyone

with an bank account has one of these and also most people use it more or

less often. With the EC card, you can get money on ATM's and pay your goods

in shops and restaurant by swiping the card and entering your PIN code (no,

I don't go into that) like an credit card but the amount is deducted

directly and immediately from your bank account.

Now on Saturday 23 Dec 2000 at 13:15, a tape robot in an automated tape

library in the data center of Telekurs, the sole operator of all EC card

transactions, drops a tape on the floor which in turn leads to an error

propagation which shuts down the whole EC and MasterCard card processing for

approximately two and a half hours until 15:25.

The impact was quite unpleasant: thousands of frustrated people unable to

pay the Christmas presents for their loved, high revenue losses for the

shops on the most important day of the year and more than 100,000 transactions rejected.

What do we learn from this? The usual story: don't put all your eggs in the

same basket; have better failure recovery procedures in place for such an

important system, it should not be possible that a dropped tape brings the

processing of all transactions to a grinding halt.

For reference coverage by the media (in German):

[http://archiv.nzz.ch/books/nzzmonat/0/\\$72NB6\\$T.html](http://archiv.nzz.ch/books/nzzmonat/0/$72NB6$T.html)

Andre Oppermann

---

## ✉ **Re: The Chinook Crash ([Risks 21.18-19](#))**

"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>

*Wed, 10 Jan 2001 13:09:16 +0100*

O'Connor ([Risks 21.18](#)) and Payne ([Risks 21.19](#)) have recently discussed the 1994 RAF Chinook transport helicopter crash on the Mull of Kintyre. And then there is Ryan O'Connell's contribution, of which more later.

This is a very public discussion in the UK. It is said to be the first time that the Royal Air Force has put an accident report in the public domain (J.M. Ramsden, "RAF Safety after Chinook", Pilot, November 2000, p22) and the controversy is sufficiently well developed for the UK defence minister at the time of the accident, Sir Malcolm Rifkind, to have requested one of his successors, Geoffrey Hoon, to set aside the finding of gross negligence reached by Sir William Wratten (op. cit., p23). It is probably the first time ever that an Air Chief Marshall with authority to determine an accident finding has written an article in the "popular" aviation press to explain his finding (Air Chief Marshall Sir William Wratten, "Why those Chinook pilots were `grossly negligent'", Pilot, August 2000, pp20-21).

Here is a brief description of the controversy. The Kintyre peninsula is long, narrow, hilly (one hesitates to say "mountainous") piece of Scotland whose end, the Mull of Kintyre, attains a height of 1404ft MSL (above mean sea level) and is some 20km (13 miles) or so across the North Channel from the nearest point of Northern Ireland. There is a lighthouse on the west side of the Mull, directly below the "peak" (Ordnance Survey, Routemaster Series, Number 3, Western and Central Scotland, ISBN 0-319-23003-1).

The flight was performed under a Visual Flight Rules (VFR) flight plan. Visual flight was performed over the North Channel. Close to the lighthouse on the Mull, the aircraft flew into Instrument Meteorological Conditions (IMC) and hit ground at 810 feet, some 2,000ft below Instrument Flight Rules (IFR) Safety Altitude for this sector of the planned route, calculated to be some 2,800ft MSL, at a groundspeed calculated by the Air Accident Investigation Branch to be some 150kts (Wratten, op. cit., p20. 1 knot (kt) is 1 nautical mile (nm) per hour; 1 nautical mile is about 1.15 statute miles).

The aircraft was equipped with a "SuperTans" GPS-based navigation computer (Ramsden, op. cit., p21), and a VFR flight plan waypoint change was made, to a waypoint some 87nm beyond the lighthouse, less than one nm from what was to be the point of impact (Wratten, op. cit., p20).

The accident flight was equipped with neither a flight data recorder nor a

cockpit voice recorder. All parties to the controversy agree that we can never know exactly what happened or why. We want to know why those highly trained and experienced pilots flew into IMC on a VFR flight plan, and why they did not perform regulation and trained maneuvers for such an eventuality (slow down, climb immediately to at or above IFR Safety Altitude for that sector, and immediately initiate a turn away or a 180-degree reversal of course out of the IMC and back into the Visual Meteorological Conditions (VMC) from whence you have just come. Wratten, op. cit., p20). We shall never know the answers to these questions.

Flying into IMC while under VFR is one of the biggest killers of general aviation pilots and their passengers. It also kills lots of professional "bush" pilots in places such as Alaska. Every pilot, \*every pilot\*, including students, is explicitly trained both to avoid doing that, and in what to do if you do it anyway (namely, the maneuvers described above, which are universal).

The Chinook helicopter, known as an HC.2 in UK military service, is a twin-rotor heavy transport helicopter. It has one rotor fore, just behind and over the cockpit, and one rotor full aft of the long fuselage. The HC.2 has a history of engine control system malfunctions (it is equipped with Full Authority Digital Engine Control, FADEC), including uncommanded "run-ups" (Ramsden, op. cit., p21). I take this to mean either an uncommanded increase in power output or an uncommanded increase in rotor RPM or both, but I don't know the exact history. Ramsden refers to

## Squadron

Leader Bob Burke, an RAF Chinook test pilot who has experienced "uncommanded HC.2 rotor runaways" (op. cit., p23). Furthermore, on the day of the accident flight, one of the flight crew asked groundcrew to check the navigation computer for "unusual GPS satellite tracking data. This check was completed with 'no fault found'" (Ramsden, op.cit., p21).

RAF Rule AP.3207.8.9 requires that there be no doubt in the case of a finding of pilot negligence (Ramsden, op.cit., p21).

The controversy is briefly as follows. ACM Sir William Wratten asserts that there is no doubt that the pilots flew into IMC conditions on a VFR flight plan, and that there is no evidence of any technical malfunction which could have caused them, against their training, to do so. His most reasonable critics believe that there is indeed such doubt: for example, an uncommanded run-up of the sort previously seen on the HC.2 could have caused the flight pattern out of VMC into IMC and impact with the Mull (for example, Ramsden, op. cit., p23, cites specific critics and an article in Pilot, October 1999, which I have not read). Sir William replies that there is incontrovertible evidence that the decisions and action of the pilots that led to flight into IMC occurred independently of the occurrence of any such technical problem or other factors presumed by some critics to be relevant (Wratten, op.cit., p21).

Much of the debate centers on the nature of RAF accident investigation

procedures, the nature of doubt and what kinds of considerations and evidence lead to it (the nature of hypothesis, plausibility, and their place in accident reports), the nature of justification and sufficient justification under conditions of uncertainty, the purpose of accident reports according to the RAF and whether the RAF's finding in this case fulfills that purpose, whether there is a "culture of blame" in RAF incident investigations, whether certain kinds of potential evidence was ignored, and whether it should have been, and the effects of the finding on military personnel as well as bereaved families, as well as the nature and role of secrecy and openness in accident investigations.

I believe that civil societies need to consider such issues, and it is clear that the RAF investigators and their commanding officers, as well as their more reasonable critics, are acting in good faith and the controversy is intellectually serious. I believe the debate is socially healthy. But then I would, wouldn't I, given my interests in the analysis of complex system failures? Well, not inevitably. I contrast the Chinook debate with that over the 1988 Airbus A320 accident at Habsheim, on which debate I have expressed my views, based on a first-level Why-Because Analysis, elsewhere (Section 5 of "Causal Reasoning About Aircraft Accidents, pp 344-355 of Computer Safety, Reliability and Security, Proceedings of the 19th International Conference, SAFECOMP 2000, ed. Koornneef and van der Meulen, Lecture Notes in Computer Science, Volume 1943, Springer-Verlag, Berlin, Heidelberg, New

York, 2000).

Back to the RISKS contributions. O'Connell ([Risks 21.19](#)) seems to believe that the distinction between VFR and IFR doesn't exist for the UK military, that the pilots "would have" been operating under some other unspecified flight rules than VFR or IFR, that they were using terrain-following radar, and that it is OK to perform terrain-following flight in IMC in the vicinity of steeply-rising terrain, and that they might well have been doing that because they were worried about anti-aircraft fire from terrorists.

Whereas O'Connor's and Payne's intellectual VFR has kept them and RISKS readers well clear of clouds, O'Connell is flying, thankfully solo, into IMC. Lighthouse keeper PGN, observing right on the border between VMC and IMC, failed to notice despite his sense of smell that O'Connell was flying directly into the Mull. It remains for our moderator only to explain the pun.

Peter Ladkin

---

## **✶ Re: Chinook (Risks-21:18 and Risks-21:19)**

Mike Beims <mbeims@mail-fair.ivv.nasa.gov>

*Thu, 11 Jan 2001 16:18:49 -0500*

The current debate about the June 2nd 1994, RAF Chinook Flight ZD 576 crash

into the Mull of Kintyre centers on the Full Authority Digital Engine Controller (FADEC) used by that helicopter. The FADEC was built by the Textron company.

In Risks 21:18 John O'Connor makes a case for Controlled Flight Into Terrain due to pilot error compounded by weather factors.

In Risks 21:19 Phil Payne makes a case that an additional risk was not having a recording of the flight data.

Also in Risks 21:19 Ryan O'Connell makes a case that a risk mitigator for low level flight in fog is the on-board terrain following radar and the military pilots training for "Nap of Earth" flying. My understanding is that even with radar, "Nap of Earth" flying is a high workload activity.

A search of the United States' National Transportation Board's (NTSB) Aviation page:

<http://www.nts.gov/Aviation/Aviation.htm>

found three FADEC related helicopter crashes, and also the fact that the

FADEC itself permanently records some flight data.

The accidents are:

(1) FTW96LA395; September 21, 1996, a Bell 407 helicopter; registration:

N1114S

(2) MIA97RA005; OCT-09-96; a Bell 407 helicopter; registration: N1117P

(3) FTW97RA055; NOV-20-96, a Bell 407; registration: ECGJC

Note the closeness of the dates and two of the registrations.

All of these crashes were considered pilot error. Readers of

this forum may recognize a human factors risk in the interface and procedures for recovery from FADEC failure. From the FTW96LA395 accident report:

"According to the Bell 407 Rotorcraft Flight Manual, when the FADEC FAIL warning light illuminates in flight, the pilot should accomplish the FADEC FAILURE procedure as prescribed in paragraph 3-3-K. The procedure is, immediately retard the throttle and hold it to the 90% throttle bezel position; maintain Nr (rotor) with collective only; depress the FADEC MODE switch one time regardless of switch indication, FADEC will switch to MANUAL mode 2 to 7 seconds after this action if it is not already in manual mode; maintain Nr 95% to 100% with throttle and collective; land as soon as possible, and perform a normal shutdown if possible. There is a warning that 2 to 7 seconds after the FADEC FAIL warnings, FADEC may be in MANUAL mode without any pilot action. Nr may increase very rapidly and overspeed to 110% which will result in an engine flameout unless the pilot takes immediate manual control of the FADEC with the throttle."

The fact that FADECs have a permanent record of their data comes from the Statement of Mike Poole to the Transportation Safety Board of Canada speaking about the September 2nd, 1998, SwissAir MD-11 crash off Peggy's Cove: "the FADEC from the Number 2 engine gave us data in those last six minutes of the flight where the recorders had already stopped. So, in this case, the non-volatile memory was extremely useful."

<http://www.nts.gov/events/symp%5Frec/proceedings/may%5F3/>

[sessioni/poole%5Ftranscript.htm](#)

The procedure for recovering from failure, the risk of engine failure if the procedure is not followed and the existence of non-volatile memory in the Textron FADEC are confirmed by the Bell Helicopter/Textron website:

[http://32.97.252.12/print/encyclopedia/407pdb/section1/page\\_1\\_123.html](http://32.97.252.12/print/encyclopedia/407pdb/section1/page_1_123.html)

A probable cause for the June 2nd 1994, RAF Chinook Flight ZD 576 crash into the Mull of Kintyre may include a human factors risk in the interface and procedures for recovery from FADEC failure. This would be aggravated by a high workload flight regime. Data for whether or not there was a FADEC failure should have been available in the non-volatile memory built into the FADEC.

Mike Beims <mbeims@ivv.nasa.gov>

---

## **✂ Armchair Chinook RISKS analysis is misplaced**

"Nathan K. Pemberton" <nate.pemberton@lmco.com>

*Wed, 10 Jan 2001 09:59:59 -0800*

In my opinion, the armchair analysis of the Chinook crash by RISKS participants is a pointless exercise. The military does not operate in a risk-free environment. They regularly take on risks which would be unacceptable to the general public. This does not imply that they should be

absolved in cases of recklessness, but the tone of the discussions so far seems to be alarmist. For a bunch of computer jocks to try to tell the military its business when it comes to operations is the height of arrogance.

For a picture of the types of risks involved in military helo ops, read the book "Black Hawk Down" by Mark Bowden. Not having served in the military myself, I cannot attest to its accuracy, but it was well received by soldiers involved in the actions described. Some of the book also appears with supplementary material on the Philadelphia Enquirer web site:

<http://www.philly.com/packages/somalia/>

Nathan Pemberton <nathanp@ix.netcom.com>

---

## **✶ Since when is Northern Ireland considered a war zone?**

Chris Warwick <chris.warwick@alcatel.com>

*Wed, 10 Jan 2001 13:08:48 -0500*

Re: Chinook (O'Connell, [RISKS-21.19](#))

The Officer in Charge has been held responsible, he/she died in the crash.

Given that the Board of Inquiry does not indicate that the aircraft was

under ground control, I presume that someone on board, likely the pilot, was

the Officer in Charge, and made the decisions that lead to the crash.

A Military Board of Inquiry is made up of both peers and superiors of the Officer in Charge. The function of the Board is to examine all the factors leading to an incident, and to examine whether the Officer in Charge made correct or reasonable decisions along the way. In this case the Board has evidence that decisions made and risks taken were NOT appropriate for the threat environment.

The Captain usually goes down with his ship, whether he/she lives or dies is a separate matter.

The risk is we overlook a potential cause for future problems, because this ruling implies that the aircraft operated flawlessly.

In this case the "cause" of the accident is clear, but we may still need to examine why the aircraft intersected the ground. If for no other reason than to make future Nape-Of-The-Earth operation as safe as it can be...

---

## **✶ Oregon Jurors summoned for 1901**

Aydin Edguer <aedguer@silverbacktech.com>

*Thu, 11 Jan 2001 18:24:38 -0500*

In Multnomah County, Oregon, about 3000 residents have been summoned to show up for jury duty in 1901. One person responded that he couldn't possibly get there in time because he had not yet been born. [Source: Michelle Roberts, \*The Oregonian\*, 3 Jan 2001; PGN-ed]

## ⚡ Y2K bug in Millennium clock

<mspalmer@mmm.com>

Wed, 10 Jan 2001 12:14:11 -0500

I received one of those countdown to the millennium clocks for Christmas 1999. It counted down the days/hours/minutes/seconds to Jan 1, 2000. When it reached zero, the displayed stayed at all zeros and flashed.

Everything worked great. It has a mode function that you can get it to count down to Jan 1, 2001 (they call this scientific mode as opposed to celebration mode). After New Years 2000, I set it to scientific mode and forgot about it. A couple of days before New Years 2001, I dug the clock out and noticed that the count down was off by a day. It was displaying 1 day and several hours to new years on Dec. 29th. I figured that it had lost a day sitting in my drawer. When I checked the actual day (you can set it to be just a date/time clock as well), it was correctly set to Dec. 29th. It turns out that the date/time software/firmware correctly dealt with leap year 2000, but the countdown code missed the boat. It must have been hard coded to count down to Jan 1, 2000, and then they probably added 365 days for the count down to 2001.

My Millennium clock has a millennium bug.

Mike Palmer

## ✉ Re: 54 weeks in a year? ([RISKS-21.18](#))

"o-Dzin Tridral" <TridralO@Cardiff.ac.uk>

*Fri, 12 Jan 2001 12:44:50 -0000*

Doesn't the problem of 54 weeks in a year depend on how week numbers are calculated?

The problem of 54 weeks seems to depend on starting weeks on a Sunday and counting Week 1 as being the week containing 1st January. Hence in the case of 2000 you get a Saturday fragment in Week 1, 52 Weeks running Su-Sa, and a Sunday fragment in Week 54.

The web page <http://www.year2000.com/y2kcurrent1.html> appears to make these assumptions.

The ISO standard for dates and times (ISO 8601) works differently by starting weeks on a Monday (that's not the important bit) and making Week 1 of a year the week containing the first Thursday. Hence week 1 of 2000 began on 2000-01-03 and the preceding Saturday and Sunday belonged to Week 52 of 1999.

I've tried to find year that has 54 weeks using the ISO definition, but failed.

The standard is at <http://www.iso.ch/markete/8601.pdf> and there are useful links from <http://www.egroups.com/group/iso8601>

I think that this standard becomes ever more important now that we're in the low year numbers of the century. We'll look back on dates like 03/05/02 and wonder what on earth it means, given the YY/MM/DD, DD/MM/YY, MM/DD/YY (and other) possible interpretations.

I hope this doesn't prove to be a weak argument and that people will be encouraged to make a date with a standard.

'o-Dzin Tridral, Senior Computer Officer, UIS, Cardiff  
University, PO Box 78  
CF10 3XL +44 29 2087 6160 TridralO@cf.ac.uk W <http://www.cf.ac.uk>

---

## ✦ Re: 54 weeks in a year? ([RISKS-21.18](#))

Paul van Keep <paul@sumatra.nl>  
*Thu, 11 Jan 2001 12:43:35 +0100*

PGN wrote: The year 2000 began on a Saturday and ended on a Sunday; ergo, 54 calendar weeks.

It is highly unlikely that week numbering was part of the cause [of the Norwegian anomaly]. Norway and the rest of Europe adheres to a different definition of the week than the US, where the week starts on Monday. There is also an ISO spec that defines week numbering. That spec states that week 1 of a year is the first week that has at least 4 days in that year. So if the year starts on a Friday, Saturday or Sunday, those first days still

belong to the last week of the year before. If we look at 2000,  
the first  
two days are week 52 (they are part of the last week of 1999)  
and 31  
December is exactly the last day of week 52 of the year.

Paul van Keep

[But some people use U.S. calendar software written by non ISO-  
aware  
folks! 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 21: Issue 21

Thursday 25 January 2001

## Contents

- [RISKS moved to new mail server and list server program](#)  
[Mike Hogsett](#)
- [Look ahead + Cache == oops](#)  
[Lindsay Marshall](#)
- [QP -> UL?](#)  
[Mark Brader](#)
- [Osprey: A Spree? Us pray?](#)  
[PGN](#)
- [Travelocity exposes customer information](#)  
[Monty Solomon](#)
- [Network Solutions exposes e-mail addresses](#)  
[Name withheld by request](#)
- [Microsoft websites blacked out -- but what happened?](#)  
[Declan McCullagh](#)
- [401k mixup](#)  
[Jeremy Epstein](#)
- [Risks of owning a cute domain name](#)  
[Griffith](#)
- [Interesting Web risk](#)  
[Lindsay F. Marshall](#)

- [Re: Organiser Bugs](#)  
[Peter B. Ladkin](#)
  - [Two-billion-dollar theft](#)  
[S Harris](#)
  - [Another Y2K+1 glitch -- sorta](#)  
[George C. Kaplan](#)
  - [Re: Millennium error, or "something like that"](#)  
[Amos Shafir](#)
  - [Re: 54 weeks in a year?](#)  
[Espen Andersen](#)  
[Bob Dubery](#)  
[Markus Kuhn](#)  
[Stan Sieler](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

## ⚡ **RISKS moved to new mail server and list server program**

Mike Hogsett <hogsett@csl.sri.com>

*Fri, 19 Jan 2001 15:07:31 -0800*

As part of the process to transition our mail server from our old, slow, dusty one to our new, fast and shiny one, we had to move all of our mailing lists to the new server. Of these lists, RISKS is the most heavily used. The list file itself contains over 7000 e-mail addresses (many of which are redistribution addresses).

During the process of subscribing all e-mail addresses to the new list, there was unfortunately a short period of time when the list was unmoderated. Inevitably, a SPAM message managed to get through! I managed to catch and stop the message before it was sent to all list members, but

unfortunately it was sent to at least 2, but not more than 1949 addresses.

[PGN: I heard from about 10 thus far.]

During the next few days, we will be tweaking the configuration for the new RISKS list. I would like to take this opportunity to apologize in advance for any hiccups we have during this process.

If any RISKS list members notice any problems with the list, please do not hesitate to e-mail me at [postmaster@csl.sri.com](mailto:postmaster@csl.sri.com) so that I can address these issue promptly. As before, all subscription and unsubscription requests should be sent to [risks-request@csl.sri.com](mailto:risks-request@csl.sri.com). For problems regarding subscription and/or unsubscription requests please send e-mail to either [postmaster@csl.sri.com](mailto:postmaster@csl.sri.com) or [risks-owner@csl.sri.com](mailto:risks-owner@csl.sri.com).

Thank you,

Michael Hogsett, System Administrator  
SRI International Computer Science Laboratory

[One of the benefits of the new majordomo service is that I will no longer have to wade through the several hundred bounces that I get on each issue. Many thanks to Mike for a major (domo arigato) effort. PGN]

---

## **⚡ Look ahead + Cache == oops**

<[Lindsay.Marshall@newcastle.ac.uk](mailto:Lindsay.Marshall@newcastle.ac.uk)>

*Wed, 17 Jan 2001 13:07:37 +0000 (GMT)*

I just received a message about an error from the RISKS Web server saying that the latest edition - named on the front page - was not a valid issue. It would seem that the request was sent through a cache through which someone had previously requested the page \*before\* it really did exist and so the error reply was cached under the name of the genuine page. The error is generated dynamically so I can't just divert the reply to a fixed page, so I will have to turn caching off on error returns. Obvious? Probably, but I didn't think of it (no surprise there then) and I haven't seen in it any lists of stupid Web programming errors!

Lindsay <<http://catless.ncl.ac.uk/Lindsay>>

---

## **⚡ QP -> UL?**

Mark Brader <[msb@vex.net](mailto:msb@vex.net)>  
*Tue, 23 Jan 2001 14:03:45 -0500 (EST)*

There have, for some years, been a number of scams whose victims are tricked into making what they think is an ordinary phone call, but actually incur surprisingly high charges some or all of which go to the scammer. Apparently an urban legend (UL) is now circulating on the Internet saying that these charges can go as high as \$2,400 per minute. This is false, but in a current thread in comp.dcom.telecom, John R. Covert says it was reported as fact (due to inadequate checking) by Boston radio station WBZ.

Linc Madison now suggests that the origin of this UL is MIME quoted-printable (QP) encoding. We've probably all seen this at some time: any character that "might not get transmitted correctly" turns into an = sign followed by two characters giving its numerical value in hexadecimal; for example, if you spell "role" with a circumflex accent in ISO 8859-1, it becomes "r=f4le".

Messages containing QP are supposed to be identified by MIME header lines that say so, and restored transparently to their 8-bit form by one's news or mail reader. But some people use older software that doesn't understand MIME. And sometimes a message gets quoted in QP form with the header lines stripped off. This is especially likely to happen with a repeatedly forwarded message like an Internet ULs -- or in a digest environment like Risks.

Now \$ is not usually considered a character that might not get transmitted correctly, but it *is* special to UNIX shells, so someone might cautiously configure it to be encoded. And what's \$ in hexadecimal, in ASCII and the ISO 8859 character sets? 24. So, as Linc says, "Thus \$25/minute turned into =2425/minute, which some helpful human turned into \$2425/minute. If you ever see a spam claiming \$242,425/minute, just remember you saw it here first."

(British pounds have a similar problem to a lesser degree. The pound sign in ISO 8859-1 is hexadecimal A3, so in similar circumstances 25 pounds could

turn into 325 pounds. I think a case of this actually has come up in Risks.)

Mark Brader, Toronto <msb@vex.net>

---

## **✶ Osprey: A Spree? Us pray?**

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

*Thu, 25 Jan 2001 10:00:36 PST*

A U.S. Marine commander has admitted falsifying the maintenance records of the tilt-rotor V-22 Osprey squadron, which has long been plagued with problems and whose development has been highly contentious throughout the previous two decades. (See [RISKS-11.94](#), [11.96](#), [12.13](#), [12.15](#), [12.40-42](#), [12.60](#), [12.73](#).) The doctored records include assigning flight-worthy indications to Ospreys that could not fly, presumably in an attempt to justify the viability of the aircraft. This is of particular concern following the two crashes in 2000 (in which 23 marines died). (See [RISKS-21.14](#).) [Source: Article by Elizabeth Becker and Steven Lee Myers, *\*The New York Times\**, 20 Jan 2001, National Edition p.A7; PGN-ed]

---

## **✶ Travelocity exposes customer information**

Monty Solomon <monty@roscom.com>

*Tue, 23 Jan 2001 00:14:10 -0500*

A security breach at Travelocity recently exposed the personal information of up to 51,000 online travel company's customers who had participated in a site promotion. Customer names, addresses, phone numbers, and e-mail addresses were revealed because of an inadequately protected directory -- possibly for up to a month. This resulted from new servers cutover from San Francisco to Tulsa. [Source: Troy Wolverton, CNET News.com, 22 Jan 2001  
<http://news.cnet.com/news/0-1007-200-4564919.html>]

---

## **✶ Network Solutions exposes e-mail addresses**

<Name withheld by request>

*Thu, 25 Jan 2001 10:04:44 PST*

You'd think they'd know better. Network Solutions, which issues most .com, etc. domain names, sends promotional mail to the e-mail addresses of domain holders. They include a URL for the recipients to use to remove themselves from that mailing list. If you use that URL, it replies that "<associated email address> has been removed".

However, the URL uses a simple "id=NNNNNNNN" field to specify the name to remove, apparently with no validation. Not only could someone easily rig up a program to run through all IDs sequentially and remove each one from the Network Solutions mailing list, in the process it would also be possible to gather the e-mail addresses of the accounts involved, which

could provide  
a wonderful mailing list for targeted spams.

---

## **Microsoft websites blacked out -- but what happened?**

Declan McCullagh <declan@well.com>

*Wed, 24 Jan 2001 16:30:58 -0500*

Millions of people have been prevented from visiting dozens of  
Microsoft

websites today. [For extensive discussion on this, visit  
Declan's Web site:

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

with background at

<http://www.politechbot.com/p-01662.html>

To subscribe to POLITECH, visit

<http://www.politechbot.com/info/subscribe.html>

See also a later report:

<http://washingtonpost.com/wp-dyn/articles/A40787-2001Jan24.html>

PGN]

---

## **401k mixup**

Jeremy Epstein <jepstein@acm.org>

*Wed, 24 Jan 2001 07:49:37 -0500*

Off by one errors are common. Another one just caused people to  
get the

wrong 401(k) statements, disclosing information like social  
security

numbers, birth dates, and balances to the wrong person. This  
has occurred

before: see [RISKS 19.26](#) for example, with a posting by an

anonymous  
correspondent .

See <http://washingtonpost.com/wp-dyn/articles/A36460-2001Jan23.html>

--Jeremy

---

## ⚡ Risks of owning a cute domain namei

<griffith@olagrande.net>

*Mon, 15 Jan 2001 04:20:13 -0600 (CST)*

As owner of the domain "dweeb.org", I find myself receiving more than my share of spam. Upon casual inspection, it seems this is no accident.

In the process of registering for various Web sites or software usage, it appears that certain people have been avoiding spam by claiming that their e-mail addresses are "dork@dweeb.org", "schmucku@dweeb.org", and similar variants.

---

## ⚡ Interesting Web risk

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

*Sat, 20 Jan 2001 20:34:31 +0000 (GMT)*

A quote from a message sent to a list I am on:

>Or HTML being rendered automagically without some restriction of  
>functionality, even if *\*that\** is done within tcl/Tk instead of

an  
>external program. (Think "Web bugs". When some scientific  
conference  
>requested that submissions be sent in HTML, I used a <BODY  
BACKGROUND=>  
>pointing to my Webserver and presto, not only did I see in the  
Web logs  
>who was refereeing my paper - highly confidential info, as far  
as  
>confidentiality goes in academia -, I could even tell how  
thoroughly  
>they had read it in the first place!! 8-} )  
>  
>(To add insult to injury, when these guys confirmed receipt of  
>submissions, they sent Word \*.DOC's, which included a list of  
the last  
>ten files loaded into Word - and they had chosen to name the  
files by  
>submission number \*and contact author\*. Oooooooops again - the  
names of  
>authors whose papers were rejected are the \*other\* confidential  
data in  
>scientific conferences ... Oh, did I mention that the first  
version of  
>their Call for Papers read "please send HTML, double spaced, no  
more  
>than ... pages"?)

---

## ✶ Re: Organiser Bugs

"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>

*Wed, 10 Jan 2001 02:20:12 +0100*

Kamens [[RISKS-21.19](#)] in reply to Berman [[RISKS-21.18](#)] asked:

>>About 4 years of notes and phone numbers lost (yes you can  
back it up

>>to a computer - The backup kit cost about the same as the

organizer).

>

> And what is the "cost" of reconstructing the four years of notes and

> phone numbers? I can't imagine that it's less than it would have cost

> to buy and use the backup kit.

The answer misses the point (I had considered a more forceful formulation of the same assertion).

I suffered a disgraceful degradation of my Palm III over, I guess, about 3 months. I'd been using it for about 2 years, had become reliant on it, and backed it up regularly. My backup was purely that, and had no GUI, because it was Linux freeware recompiled for Solaris. I wanted just a backup, not a computer interface to the Palm.

The Palm quit one day. Soft reset didn't reset. Hard reset didn't work.

Dead. I went home. First problem I had ever seen in two years of operation. Two hours later, I found that indeed my hard reset appeared to

have reset the device. I reloaded it from backup. No calendar entries from

the last 3 months (disaster: some of them were vital for legal proceedings). None of the recent entries in my address db were there. I

looked at the file modification dates on the backup machine.

Many had not

been modified for months, despite my regular backups; even those which

showed more recent modification dates appeared to have older data.

The on-screen notifications "<filename> backed up" (or whatever it was) had

just been lies, for an indeterminate period of time. This is not hard to

understand. But when it happens to you, it is cognitively hard to believe.

There is no simple way to duplicate paper-based algorithms. Whatever you have on paper, you can photocopy once a month and keep somewhere else, and you are guaranteed that the original and the copy remain unaltered; if one disappears, you know it right away and can use the other.

Try to duplicate that with a computer. Suppose I had had what I missed: a GUI interface to the backup. The GUI shows me a tiny fragment of one largeish database at a time. What would it take for me to tell that something was missing, and that that was not the only thing missing, and that each time I backed up, something more went missing? What would it take for me to notice that the db had remained approximately static, although I had made new entries (maybe the new entries were there, but consider behavior in which new entries were made at the expense of older ones)? Exactly what algorithm would you suggest that I use to ensure my digital organiser plus backup had the same or better trustworthiness properties as my paper version?

Much, even most, of the discussion on recovery from failure of computer-based processes assumes that the failure is catastrophic, sudden, and overtly remarked, and that previous states were veracious. In other words, that the computer system breaks just as a tire punctures. Well, that's not the way things always work. Digital systems also fail "live", and that is not just theory.

I spent some years seriously trying to develop paper-free work. Now, everything remotely important to me goes on paper, even when written on a machine. For much of it I ensure there are two spatially separated paper copies. I mostly use the paper copies for backup; even on-line backup via scanners. it isn't perfect, but I recommend the practice, and shall continue to do so until someone offers me usable algorithms for digital devices with properties at least as durable as those of the paper-based ones they will replace.

PBL

---

## **⚡ Two billion dollar theft (Re: CIOs: "What, Me Worry?" [RISKS-21.19](#))**

S Harris <sharris@operamail.com>

*Fri, 12 Jan 2001 02:10:48 -0500*

>> ... Meanwhile, a 1999 survey found that Fortune 1000 companies lost  
>> more than \$45 billion in thefts of proprietary information that  
>> year. [*\*InfoWorld\**, 3 Jan 2001; NewsScan Daily, 4 Jan 2001]

In [RISKS-21.19](#) Mark Hull-Richter writes:

> I am HIGHLY skeptical of all claims of losses by large corporations.  
> How does this \$45 billion number come about? How does a company arrive  
> at the amount of money they actually lost due to theft of

proprietary  
> information?

I can give a first hand account of a \$2 billion theft of proprietary information to illustrate how these exaggerated figures get manufactured.

Back in 1989 I worked at a Toronto software development company that did lots of work with the Unix operating system, and licensed the Unix source code from AT&T for about \$60,000 a year.

Night after night someone was logging in to the computers from a dialup line to download chunks of the Unix source code. Somebody at the company noticed this, called in the police, who traced the connection to an ex-employee, raided his house and seized his home computer. Apparently the ex-employee, a software development manager, who had recently left the company, missed having access to the Unix source code and wanted to grab a copy of it for personal study. Satisfied that the source code had been recovered, and that this wasn't a case of espionage or sabotage, the company would have been happy to let the matter drop.

But the cops insisted on laying charges and it appears that they leaked the story to the media. All three Toronto newspapers (Toronto Sun, Toronto Star, and the Globe & Mail) reported that the police had foiled a \$2 billion theft!

Why wasn't this as a \$60,000 theft of a commercial source code license?

Or at the very most a \$500 theft of an educational license, since the ex-employee's intended use was only to study it?

Well it seems that the police had called up AT&T and asked them "How much is Unix worth?" The answer was \$2 billion. AT&T gave Unix an asset value of \$2 billion on their books. The police equated a little mischief to the cost of acquiring total ownership of AT&T's Unix System Laboratories and all its intellectual property!

In this case, the large corporation gave an accurate estimate to a bogus question. It was law enforcement (and sloppy fact checking by the media) that twisted the story.

But you know, even the \$2 billion asset value seems suspect to me now because AT&T sold Unix to Novell in 1993 for just \$270 million (see <http://www.att.com/press/0693/930614.ulb.html>). Novell in turn sold it to SCO in 1995 for a paltry \$54 million (6M SCO shares at about \$9 each is \$54M, see <http://www.novell.com/company/ir/96annual/mandis.html>). But if AT&T overestimated by tenfold, the police still exaggerated by 4 million fold.

---

## ✶ Another Y2K+1 glitch -- sorta

"George C. Kaplan" <gckaplan@ack.berkeley.edu>  
*Thu, 18 Jan 2001 14:59:50 -0800*

The Extreme Ultraviolet Explorer (EUVE) satellite was launched in Jun 1992 to do astronomical observations in the extreme ultraviolet (100

- 1000 angstroms). Its primary mission was planned for something like 18 months, but a series of extensions has kept the satellite running ever since, operated by UC Berkeley and NASA. Money is finally running out, and it's scheduled to shut down on 31 Jan 2001.

On 1 Jan 2001, a planning system that checks observing plans against operational constraints suddenly failed. A Y2K+1 bug? Not quite. Many of the constraints are based on the relative positions of the sun, moon, and planets. (e.g. "Don't point the telescopes at the sun.") A solar/lunar/planetary (SLP) ephemeris file which provides this information to the planning system was valid only through 31 Dec 2000.

OK, someone forgot to do the annual update, right? Nope. Solar system motions are well-known and predictable over long time periods. The SLP file covered a 10-year period; it was the only one ever used by the mission. No provision was made for updating the file, since at the time EUVE was launched, nobody expected the mission (even with extensions) to last through 2000.

So it's a classic problem of legacy software and data. The original programmers are long-gone. Nobody knows quite where the original file came from, and the (binary) format is different from SLP data used on more recent missions operating with similar constraints.

At this point it's unlikely that an updated file will be available before the mission shuts down, so the operations team at UC Berkeley is

just  
bypassing the SLP checks. That's a risky choice, but  
reasonable, given that  
they have only a couple of more weeks of operations. You have  
to wonder  
what they would have done if the mission had been extended for  
another year,  
though.

George C. Kaplan, Communication & Network Services, University  
of California  
at Berkeley 1-510-643-0496 gckaplan@ack.berkeley.edu

---

## **[Re: Millennium error, or "something like that" \(Jacobsen, RISKS-21.19\)](#)**

Amos Shafir <AmosS@sphera.com>  
*Thu, 18 Jan 2001 09:26:51 +0200*

Well, Flex doesn't know about such a rule mainly because there  
isn't one;  
the Gregorian leap year rules are just for 4/100/400 years, no  
1000-year  
rule (nor 4000 or 10000, which I have also heard about). In  
this note  
at least it's quoted as "something like that", but such errors  
have also  
found their way into code, such as the PostScript code quoted in  
the note  
by Eric Lindsay which immediately followed the one above in  
[RISKS 20.19](#);  
I wouldn't be surprised to find out that such code was  
responsible for  
some Y2K bugs (it seems not all of them have been discovered  
yet).

The RISK here of course, that of generating code out of  
algorithms that

the programmer knows at "something like that" level, instead of taking the trouble to check out the facts before coding.

Amos Shapir <amos@sela.co.il>

---

## ✉ **Re: 54 weeks in a year? ([RISKS-21.18](#))**

Espen Andersen <self@espen.com>

*Sun, 14 Jan 2001 05:38:49 +0100*

The discussion of the Norwegian State Railway (NSB) troubles with the 2000/2001 transition focuses on fairly advanced causes, such as the 54-week situation. The discussants (including our esteemed moderator) seem by this to believe that the NSB is a competent and responsible organization. As recent events (such as a horrible rail accident with 19 dead where it turned out the railroad had a number of Single Point of Failure situations, or the fact that the new high-speed "Signature" trains had been built with axles that cannot tolerate high speeds and turns at the same time) has shown, this organization has completely lost the public's confidence (as witnessed by the recent, forced departure of its CEO), as has its locomotive supplier ADTranz.

My hypothesis is that the 2000/2001 bug was a regular millennium bug, found in 1999. The problem was then "fixed" by turning the clock back one year to buy time, and promptly forgotten. Now NSB and

ADTranz has turned back the clock back once again. This time, with the newspaper and RISKS interest, they are unlikely to forget.

Espen Andersen <self@espen.com>, Norwegian School of Management (www.bi.no)  
+47 6755 7177 European Research Dir., The Concours Group www.concoursgroup.com

---

## ✶ Re: 54 weeks in a year?

"Bob Dubery" <bdubery@netcare.co.za>  
*Mon, 15 Jan 2001 08:35:48 +0200*

Standards are great - but it's RISKy to assume that they are being adhered to just because they're published and sensible.

I led a y2k remediation project in 1999. I saw the source code for literally thousands of programs. Some code anticipated a leap year, but never exactly to the standards (IE the code would have accepted 1900 as a leap year). Very seldom were date and time presented in any kind of standard format. I'm willing to bet that if I asked all the programmers at my office what ISO and RFCs are not all of them would know about ISO, and less than half would have heard of RFCs - and nearly all of them wouldn't see the point.

This sounds disparaging, I know. I'm a programmer myself, so I do know whereof I speak. I never worked for an employer that stipulated adherence to any ISO standard. I have dealt with 3 "Web design houses" who

had no  
knowledge of RFCs.

If standards had been adhered to then why did we have a Y2k  
problem? And why  
do we know have systems unable to roll into 2001?

---

**✉ Re: 54 weeks in a year? (Tridal, [RISKS-21.20](#))**

Markus Kuhn <mgk25@cl.cam.ac.uk>  
*14 Jan 2001 12:07:49 GMT*

> I've tried to find a year that has 54 weeks using the ISO  
definition,  
> but failed.

A detailed discussion of the ISO 8601 international date and time  
notation standard, including a proof for why years can only have  
either 52 or 53 weeks according to the international standard  
week  
numbering scheme, can be found on

<http://www.cl.cam.ac.uk/~mgk25/iso-time.html>

ISO 8601 has been adopted as a national standard in quite a  
number of  
countries over the past few years and it seems to enjoy rapidly  
increasing popularity. Computer experts should definitely make  
themselves familiar with it.

Apart from standardizing a consistently bigendian numeric date  
and time  
notation, it should also encourage in particular US users to  
finally  
give up the awkward, error prone, risky, ambiguous and  
inefficient am/pm  
time-of-day notation in favour of the modern and elegant  
international

standard 00:00-23:59 notation.

The antique 12h am/pm notation that is still so widely used in the US

even in airport time tables has \*many\* disadvantages like:

- It is longer.
- It takes somewhat more time for humans to compare two times in 12h notation.
- It is not clear, how 00:00, 12:00 and 24:00 are represented. Even encyclopedias and style manuals contain contradicting descriptions and a common quick fix seems to be to avoid "12:00 a.m./p.m." altogether and write "noon", "midnight", or "12:01 a.m./p.m."+ instead, although the word "midnight" still does not distinguish between 00:00 and 24:00 (which are the standard notations for midnight at the start and at the end of a specified day).
- It makes people occasionally believe that the next day starts at the overflow from "12:59 a.m." to "1:00 a.m.", which is a quite problem not only when people try to program the timer of VCRs for shortly after midnight.
- It is not easily comparable with a string compare operation, so it doesn't automatically sort correctly in alphabetical listings.
- It is not immediately obvious for the unaware, whether the time between "12:00 a.m./p.m." and "1:00 a.m./p.m." starts at 00:00 or at 12:00, i.e. the am/pm notation is certainly more difficult to understand.

I don't understand, why in the US only the military and computer programmers see the many obvious advantages of the modern standard time notation. Perhaps the somewhat odd way of pronouncing the

full

hours in US English as "eighteen hundred", which the US military seems to have introduced, as opposed to the more natural "eighteen o'clock" for 18:00 might have scared the civil world from adopting it as well.

Those interested in the above might also want to read the neighbour Web page

<http://www.cl.cam.ac.uk/~mgk25/iso-paper.html>

It describes another well-established highly elegant global standard that could -- if it were finally also adopted in the US and Canada -- eliminate a long list of risks and inconveniences in international document exchange and in the use of photocopying machines: A4 paper.

Markus G. Kuhn, Computer Laboratory, University of Cambridge, UK  
mkuhn at acm.org <<http://www.cl.cam.ac.uk/~mgk25/>>

---

## **⚡ Re: 54 weeks in a year?**

Stan Sieler <sieler@allegro.com>  
*Mon, 15 Jan 2001 11:21:50 -0800 (PST)*

Re:  
> Doesn't the problem of 54 weeks in a year depend on how week numbers are  
> calculated?

Of course it does! Our modified paper, at  
<http://www.allegro.com/papers/54.html>,  
makes that clearer than the original version. Unfortunately,  
version 2.0

of the paper never got posted at year2000.com.

> The ISO standard for dates and times (ISO 8601) works differently by  
> starting weeks on a Monday (that's not the important bit) and making Week 1

Yep. But, as we point out, standards don't matter if you're doing it differently. And, some people definitely do it differently. One of our customers uses the "Sunday is first day" logic, and ran into the 54 week problem.

Stan Sieler <sieler@allegro.com> www.sielers.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 21: Issue 22**

**Friday 26 January 2001**

## Contents

- [Software crash hits Canadian grocery chain](#)  
[Aaron PooF Matthews](#)
- [Aircraft had near-miss in Finland](#)  
[Michael Walsh](#)
- [UK Trials of GPS controlled car speeds](#)  
[Steve Loughran](#)
- [Theft of vehicle leads to robbery at home](#)  
[D. Joseph Creighton](#)
- [Bank robber nabbed by GPS](#)  
[Roger H. Goun](#)
- [B of A Visa Y2K glitch?](#)  
[Ethan McKinney](#)
- [Risks of shortcuts in user interfaces](#)  
[Austin Donnelly](#)
- [Cross-site scripting still a threat](#)  
[Michael Sims](#)
- [HotMail blocking users from e-mailing Peacefire](#)  
[Bennett Haselton](#)
- [Network vandal attacks Microsoft sites](#)  
[NewsScan](#)

- [Hacker indicted for network vandalism](#)  
[NewsScan](#)
  - [Sex-offender Web sites are insecure](#)  
[Monty Solomon](#)
  - [Remote disabling of satellite TV receiver smart cards](#)  
[Jeremy Epstein](#)
  - [Shoppers seize unauthorized discounts at Macys.com](#)  
[Monty Solomon](#)
  - [Re: Palm Pilot Security](#)  
[Mitch James via Dave Stringer-Calvert](#)
  - [Clone phones with help from AT&T](#)  
[Nikita Borisov](#)
  - [Re: Chinook](#)  
[Lloyd Wood](#)  
[Ken Garlington](#)
  - [Expanding on an urban legend](#)  
[Danny Burstein](#)
  - [Re: "Security holes protect your equipment from theft"](#)  
[Daniel P. B. Smith](#)
  - [Re: Risks of mail auto-reply](#)  
[Jerrold Leichter](#)
  - [Hotmail declines to accept new users with reserved words in last names](#)  
[Robert Rossa](#)
  - [ACMI Message for RISKS Subscribers](#)  
[Lillian Israel](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

## ✶ Software crash hits Canadian grocery chain

<Aaron PooF Matthews>

Thu, 25 Jan 2001 20:54:01 -0500

<http://cbc.ca/cgi-bin/view?/news/2001/01/25/sobeys010125>

Sobeys (Canada's second largest grocery mega chain) had a

computer systems  
outage that lasted over a five day period. The result of the  
outage is that  
they will miss their projected profits.

[CBC reported that Sobeys will take an after-tax charge of  
Canadian  
\$49.9 million because it had to scrap its SAP software system.  
Dan Haggerty also noted this item. PGN]

---

## ✈ Aircraft had near-miss in Finland

Walsh Michael <michael.walsh@wmdata.fi>

*Mon, 15 Jan 2001 16:52:05 +0200*

Last week's Finnish papers were full of the continuing story of  
how a  
Russian Aeroflot plane leaving Helsinki Vantaa airport came  
within 450 feet  
of a Finnair charter flight returning from Malaga. (This  
happened in  
November 2000, but was just reported.) Apparently the Russian  
plane kept  
disappearing (and coming back) from the radar screen in the  
tower.

In the following days the plot thickened.

\* Helsinki Vantaa has since March 2000 a new modern French radar  
system.

\* Aeroflot planes have (since then) often displayed this fault.

\* Conclusion (Finnish spokesperson - day one) the problem is  
with the Russian  
planes.

\* Day two Aeroflot came back with the comment that their planes  
were flying

to many other Western European destinations and Helsinki/Finland was the only airport that had reported this problem.

\* Day three the Finnish reply was that the old planes that Aeroflot were using on the Helsinki run were old, Russian (undertone - rubbish) whereas they were using better planes in the rest of Western Europe.

Somewhere in the midst of this we had statements from the Finnish side that passengers were not at risk. Oh yes?

Given the Finnish/Russian history, we're not likely to have this thing cleared up any day soon.

I tend to **\*\*wildly guess\*\*** that as the only thing that has changed is the (French) radar system (we've had old rubbishy Russian planes on this route for years), someone should be looking at that a bit more closely. It maybe assumes newer planes than those Aeroflot use.

Anyway, the Risk: Should I choose my Finnair charter flight on the basis of whether a Russian plane is due to land or take off at roughly the same time, and how do I cater for the inevitable delayed flights on either side?

Mike Walsh, Helsinki <mnw@bigfoot.com>

[I suppose if there had been an Irish controller in the tower, the blame would have fallen on a Mickey Finn. PGN]

---

## **UK Trials of GPS controlled car speeds**

"Steve Loughran" <slo2@iseran.com>

*Fri, 19 Jan 2001 20:33:33 -0800*

From the Guardian, Saturday Jan 20, an update on the proposal for GPS speed control of vehicles, where the car determines its maximum speed from an in-vehicle database of speeds of roads.

[http://www.guardianunlimited.co.uk/uk\\_news/story/0,3604,425344,00.html](http://www.guardianunlimited.co.uk/uk_news/story/0,3604,425344,00.html)

The government has commissioned a trial of speed limiters in cars, which

could lead to computer-controlled overrides as a standard fitting within

five years. Twenty trial vehicles will be fitted with a system which has

won praise on a prototype Ford Escort driven over thousands of rigidly

monitored miles in the past three years.

The tests, which prevented the car from topping 30mph, 40mph and other

limits, were "highly reliable" according to the Institute of Transport

Studies at Leeds University, which has won funding for the expanded trials

from the Department of Transport, Environment and the Regions."

"We've had two dozen people driving along a 40 mile route, including the

A1M motorway," said Oliver Carsten, head of the project, which has also been

demonstrated on the north circular road in London.

The system uses a computerised navigator linked to the car's electronic

controls and a positioning satellite. Areas with speed restrictions are

fed into the system to trigger action as soon as a limit is breached.

Just think how much fun you'll be able to have by a UK motorway in five years time from jamming the GPS signals. Or how much a 'chipped' database or speed limiter will be worth. A more rigorous trial would be to place the speed limited vehicles in the hands of well known violators of the speed laws to see how much effort it takes to disable -- the UK home secretary himself, for example.

Steve Loughran

[Home, Secretary, and don't spare the tires. PGN]

---

## **⚡ Theft of vehicle leads to robbery at home**

"D. Joseph Creighton" <djc@cc.UManitoba.CA>

*Thu, 11 Jan 2001 11:03:09 -0600*

A laptop computer with sensitive files on high-level drug investigations was stolen from an RCMP officer's house on New Year's Eve. Apparently, the officer's van was first stolen while he was attending a hockey game. The thieves discovered his address from the vehicle registration and drove to his home where they made off with thousands of dollars in personal property and the computer. [Source: \*Winnipeg Free Press\*, 11 Jan 2001]

The risks in keeping such sensitive information at home, presumably not protected with any sort of encryption, are obvious. But I never realized

that home address information on registration papers was a risk until now.

D. Joseph Creighton [ESTP] | Programmer Analyst, Database Technologies, IST  
Joe\_Creighton@UManitoba.CA | University of Manitoba Winnipeg, MB, Canada,

---

## ⚡ Bank robber nabbed by GPS

"Roger H. Goun" <roger@bcah.com>  
*Wed, 17 Jan 2001 20:34:49 -0500*

Together with his loot, a Vancouver bank robber jumped into a taxi that was equipped with satellite tracking technology. At the request of the police, the taxi company was able to track the cab by GPS, and the police apprehended the robber a few blocks away. [PGN-ed from a Reuters item <<http://news.excite.com/news/r/010116/10/odd-taxi-dc>>]

Roger H. Goun, Senior Staff Kennel Boy, Brentwood Country Animal Hospital, P.C.  
Exeter, New Hampshire, USA

---

## ⚡ B of A Visa Y2K glitch?

Ethan McKinney <e.mckinney@attglobal.net>  
*Thu, 18 Jan 2001 11:32:26 -0800*

I had Visa card through Bank of America which I canceled last January (2000). Imagine my surprise when a bill arrived in the mail

yesterday!

Fortunately, it was for \$0.00, but I was concerned that B of A might have somehow reactivated my account. When I called their customer service number, the rep was not at all surprised by my situation. "It's a computer error. Just ignore it," she said.

Sadly, I don't have any firm proof, but I suspect this was a slow-acting Y2K glitch. If they're still using two-digit years, they might have set up the system to read "00" as "100." Noting that it's the year 01 and my card isn't going to be cancelled until 100, the computer decided to send me a bill.

Ethan McKinney, 1750 E. Appleton St. #4, Long Beach, CA 90802

---

## **✶ Risks of shortcuts in user interfaces**

Austin Donnelly <Austin.Donnelly@cl.cam.ac.uk>

*Sat, 20 Jan 2001 13:21:11 +0000*

You know how bank ATMs have those little buttons down the side of the screen to select from an on-screen menu? Mostly, they're useful: they allow only the valid options to be presented to the user, and keep the number of different buttons required down to a minimum. But ATMs also have a variety of other buttons on the keypad (usually including "OK" and "Cancel") and this split screen/keypad user interface can lead to problems.

For example, today I met young lady who was quite distressed

because she  
thought the ATM had "eaten" her card. The problem was that the  
on-screen  
menu was laid out as follows:

```
Push here for other services --> [::]  
    Press Cancel if finished      [::]
```

The poor lady was pushing the bottom (non-active) screen button,  
rather than  
reading the instructions to press a separate key. The screen  
layout here is  
not terribly helpful, since it suggests that the bottom button  
might do  
something.

But the real risk is that if you provide shortcuts to perform  
common tasks,  
then users won't learn how to do things that aren't available  
from a  
shortcut.

Austin

---

## **✶ Cross-site scripting still a threat**

Michael Sims <jellicle@inch.com>

*Tue, 23 Jan 2001 14:51:14 -0500*

News.com (CNET) unveiled today a fresh new look to their site.  
The two  
major innovations appear to be:

- a) huge, garish advertisements
- b) cross-site scripting vulnerabilities

The new site accepts URL variables - user input - for page  
titles and

headlines in the pages. This allows users with a moderate degree of savvy to "write your own CNET headlines", or write your own javascript to be executed from CNET's pages.

You can publicize URLs like this:

<http://news.cnet.com/news/topic/0-1003-249-0.html?title=CNET%20Editors%20Agree:%20Slashdot%20is%20a%20better%20news%20site%20than%20News.com&topic=slashdot>

or this:

[http://news.cnet.com/news/topic/0-1003-249-0.html?title=Breaking%20News:%20Bill%20Gates%20Commits%20Suicide%20at%20Age%2042%20-%20Survived%20by%20three%20ugly%20children%20and%20wife<script>javascript:alert\('Javascript%20is%20executed%20-Your%20Site%20is%20Vulnerable'\)</script>&topic=Microsoft](http://news.cnet.com/news/topic/0-1003-249-0.html?title=Breaking%20News:%20Bill%20Gates%20Commits%20Suicide%20at%20Age%2042%20-%20Survived%20by%20three%20ugly%20children%20and%20wife<script>javascript:alert('Javascript%20is%20executed%20-Your%20Site%20is%20Vulnerable')</script>&topic=Microsoft)

Javascript executed on the site can grab a user's cookie information or perform other nefarious tricks; since CNET has a substantial e-commerce section (auctions, shopping, jobs, etc.) this seems rather dangerous. But for a news site, "write your own headlines" could be even more damaging.

This problem was widely publicized in the spring and summer of last year (and frankly, should have been well known to Web developers long before that). In fact, CNET has several stories about the issue in their archives. It is apparent, however, that if web developers don't learn from others' mistakes, they are doomed to repeat them.

CNET was notified six hours before this e-mail was sent to RISKS; they have not replied at this time or taken any corrective action.

Michael Sims - slashdot.org editor - michael @ slashdot.org  
Your Rights Online - <http://slashdot.org/yro>

---

## ✶ HotMail blocking users from e-mailing Peacefire

Bennett Haselton <bennett@peacefire.org>

*18 Jan 2001 21:41:22 -0500*

[sent to journalists on Peacefire's press contacts list;  
RISKS saw it in a forwarding of a message from Monty Solomon]

We recently discovered that for the last five months, HotMail has been blocking their users from sending e-mail to peacefire.org addresses. If you tried to send mail to a peacefire.org address from HotMail, you'd get a fake error message a day later saying that there was a problem on the recipient's end -- when it was really HotMail blocking the message from being delivered.

HotMail is part of the same boycott that AboveNet was part of, when AboveNet was blocking their downstream users from accessing our Web site. After our ISP owner complained, HotMail stopped blocking their users from e-mailing us and other Media3 customers.

HotMail is still, however, blocking their users from e-mailing other sites on their "boycott list". I've talked to several of our members who are using HotMail, and most of them are furious that HotMail would be censoring their outgoing mail without telling them.

Again, the irony is that HotMail didn't single us out for anything, we just happened to be in the same IP address block as other sites that were the original target of the boycott (e.g. ListSorcerer.com). When our ISP, Media3, didn't kick them off, the boycott organizers expanded the "boycott list" to include hundreds of unrelated sites also hosted by Media3.

Several HotMail members that I talked to, have said they would be willing to talk to the press about HotMail blocking their outgoing mail. Many of them said they never would have signed up with HotMail if they knew their mail would be blocked, and some have even said that they're going to switch to another mail service. (Especially since HotMail is *\*still\** blocking outgoing mail -- it was just our IP address block that they exempted from the list.)

-Bennett

bennett@peacefire.org      <http://www.peacefire.org>  
(425) 649 9024

- - -

The Telecom Digest is currently mostly robomoderated. Please mail messages to [editor@telecom-digest.org](mailto:editor@telecom-digest.org).

[Incidentally, for the mailing of [RISKS-21.21](#), bigfoot.com blocked the mailing to every subscriber there, because of the number of subscribers exceeding some spam limit. Too bad. Perhaps they won't get this message either, letting them know what happened, although we are trying a different mail configuration for this issue! PGN]

## **⚡ Network vandal attacks Microsoft sites**

"NewsScan" <newsscan@newsscan.com>

*Fri, 26 Jan 2001 08:21:59 -0700*

Just a day after Microsoft's Web sites were down for an extended period of time because of the "human error" of a technician, they were victimized by the "human malice" of a network vandal who subjected them to a "denial of service" attack that flooded them with bogus communications, causing them to gridlock and reject legitimate communications from their customers. The company has called in the FBI for assistance. Computer security expert Abe Singer of the San Diego Supercomputer Center said that part of Microsoft's vulnerability to attack was due to the fact that its four domain-name servers are linked in a single network. "They had all their eggs in one basket and basically someone knocked down the basket." (\*The Washington Post\*, 26 Jan 2001; NewsScan Daily, 26 Jan 2001  
<http://washingtonpost.com/wp-dyn/articles/A47581-2001Jan25.html>)

---

## **⚡ Hacker indicted for network vandalism**

"NewsScan" <newsscan@newsscan.com>

*Fri, 26 Jan 2001 08:21:59 -0700*

Twenty-one-year-old Jerome Heckenkamp has been indicted by

federal prosecutors for allegedly hacking into computers at eBay, Exodus, Juniper, eTrade, Lycos, and Cygnus and causing a total of more than \$900,000 in damage, in events that took place in 1999 while he was a student at the University of Wisconsin. He has pleaded innocent of all charges and says the break-ins were done by someone else using his computer. (AP/  
\*San Jose Mercury News\*, 25 Jan 2001; NewsScan Daily, 26 Jan 2001  
<http://www.mercurycenter.com/svtech/news/breaking/ap/docs/7863961.htm>)

---

## **✶ Sex-offender Web sites are insecure**

Monty Solomon <monty@roscom.com>

*Fri, 12 Jan 2001 23:08:58 -0500*

Nine state online sex-offender registries have had inadequate computer security and easily could have been hacked, an MSNBC.com investigation has found. And in two states, more general criminal records databases also were found to be insecure. The flaws put Web site data at risk and raised the possibility that a computer intruder could add or remove people from the online versions of the databases.

<http://www.msnbc.com/news/514284.asp>

---

## **✶ Remote disabling of satellite TV receiver smart cards**

"Jeremy Epstein" <jepstein@webmethods.com>

*Fri, 26 Jan 2001 14:01:03 -0500*

DirectTV has the capability to remotely reprogram the smart cards used to access their service, and also to reprogram the settop box. To make a long story short, they were able to trick hackers into accepting updates to the smart cards a few bytes at a time. Once a complete update was installed on the smart cards, they sent out a command that caused all counterfeit cards to go into an infinite loop, thus rendering them useless.

A commercial use of information warfare? Very interesting article at

<http://www.securityfocus.com/frames/?content=/templates/article.html%3Fid%3D143>

(sorry for the long URL).

Jeremy

[Reminder: As usual, no guarantee as to the future validity of URLs. PGN]

---

## **✶ Shoppers seize unauthorized discounts at Macys.com**

Monty Solomon <monty@roscom.com>

*Tue, 23 Jan 2001 00:13:26 -0500*

Macys.com was victimized by its own 50% discount coupon code that was inadvertently posted at FatWallet.com. The extent of the resulting spending spree was not divulged. "Although mistakes of this kind do

happen in the  
offline world, the speed at which e-commerce moves can make a  
small glitch  
turn into a thousand-dollar error." (Note earlier problems  
involving  
staples.com and amazon.com.) [Source: Greg Sandoval, CNET News.  
com, 22 Jan  
2001 URL: <http://news.cnet.com/news/0-1007-200-4564219.html>; PGN-  
ed]

---

## **✶ Mitch James: Re: Palm Pilot Security**

Dave Stringer-Calvert <dave\_sc@csl.sri.com>

*Thu, 25 Jan 2001 16:12:30 -0800*

PDAs considered insecure... now there's a surprise.

Date: Thu, 25 Jan 2001 15:37:10 -0800  
>From: Mitch James <mitchj@AVANADE.COM>  
Subject: Re: Palm Pilot Security  
To: PEN-TEST@SECURITYFOCUS.COM

The headline is "@stake, a US-based security consultant, has  
written a piece  
of software code that can zap passwords off targeted Palm Pilots  
through  
taking advantage of the PDA's hotsync function. Hotsync is used  
to transfer  
data between the user's PC and a Palm Pilot."

The link to the article is here

<http://www.vnunet.com/News/1116644>

Mitch James

---

## ✂ Clone phones with help from AT&T

Nikita Borisov <nikitab@espresso.CS.Berkeley.EDU>

*Mon, 15 Jan 2001 17:51:19 -0800*

I have cell service with AT&T Wireless Services in the Bay Area, and I recently purchased a new phone from them. Along with the phone, I received a 1-800 number to activate my new phone. When I called it, I reached an automated service, which asked me for:

1. My phone number
2. My 5-digit zip code
3. The ESN (equipment serial number) of my new phone.

After this, the friendly recording informed me that my account information had been updated, and the new phone should be active in half an hour. It then offered me the chance to change the ESN for any other phones. Not being in the cloning business, I declined. My new phone started working, just as they promised.

The RISKS? Given the small number of possible zip codes in, say, the 415 area code, it shouldn't take long trying zip codes and phone numbers within the AT&TWS exchanges at random before you get one right. Or surprise your friends or business partners by taking over their cell phone service and answering their incoming phone calls!

- Nikita

[Note added later in response to a comment from PGN:]

I actually received some further information from AT&T. In response to my concerns, they stated:

- 1) They have detection software that looks for sudden geographic migration (their example was a shift from Berkeley to Sunnyvale within a span of 10 minutes).
- 2) They promise that I won't be billed for an illegally changed ESN.
- 3) The incidence of such fraud is small enough for them not to take additional precautions.

I'm still a little worried about the possibility of a directed attack, i.e., someone who knows me stealing my cell phone # to find out who calls me. But there are probably other ways to do this, if you're resourceful enough...

- Nikita

---

## ✶ Re: Chinook (Phil, [RISKS-21.19](#))

Lloyd Wood <l.wood@eim.surrey.ac.uk>

Tue, 16 Jan 2001 15:55:04 +0000 (GMT)

> ... putting all your eggs in one basket - flying such a concentration of  
> critical expertise in a single aircraft was reckless

The UK electrical engineering establishment (that is, regular Institution of Electrical Engineer magazine articles, local talks, and sundry university lecturers in their dotage) will tell you in detail about the tragic life of

Alan Dower Blumlein, an electronics wizard, audio engineer par excellence,  
and all-round Good Egg, who sadly died with most of his almost-as-talented-yet-seemingly-nameless colleagues when a research plane jolly they were all taking together over England for a bit of a lark came something of a cropper during The Big One (World War II).

Oh, the loss to electrical engineering! Oh, the loss to the war effort! Oh, the many retrospective articles on Blumlein's short and tragic life! Oh, the generations of bored undergraduates! Oh, what might have been!

Half a century on, nothing has changed.

<L.Wood@surrey.ac.uk>PGP<<http://www.ee.surrey.ac.uk/Personal/L.Wood/>>

---

## ✉ Re: Chinook (Beims, [RISKS-21.20](#))

"Ken Garlington" <kennieg@flash.net>  
*Mon, 15 Jan 2001 08:31:31 -0600*

Mike Beims suggests that "Data for whether or not there was a FADEC failure should have been available in the non-volatile memory built into the FADEC."

This assumes that the FADEC memory survived the crash essentially intact. From my experience, NVMS in flight systems of this type are not crash-rated to the extent of a "real" crash recorder, and can fail in a crash.

## **✶ expanding on an urban legend, re: QP -> UL? (Brader, [RISKS-21.21](#))**

danny burstein <dannyb@panix.com>

*Thu, 25 Jan 2001 20:31:04 -0500 (EST)*

(Note that I've replaced all entries that had a USA dollar sign with the word "usads". The reason will be obvious in a bit.)

[discussion of how the legend of 2,400 dollar phone calls came about]

> If you ever see a spam claiming (usads) 242,425/minute, just remember

> you saw it here first."

Note that last line, with the "242,245/minute" comment. The original postings in comp.dcom.telecom, as well as the repost in comp.risks, used the graphical representation of a USA dollar sign.

Which, naturally, would get misread by some software so as to prepend yet another "24" to the figure.

---

## **✶ Re: "Security holes protect your equipment from theft"**

"Daniel P. B. Smith" <dpbsmith@world.std.com>

*Thu, 25 Jan 2001 18:46:05 -0500*

RISKS of technical terms with multiple meanings...

Asante, <http://www.asante.com/product/index.html>, says proudly that their routers feature "security holes." This is their term for

physical holes in  
the housing of their device, which facilitate the attachment of  
a steel  
cable so that the device can be physically secured against theft.

Daniel P. B. Smith <dpbsmith@world.std.com>  
"Lifetime forwarding" address: dpbsmith@alum.mit.edu

---

## ✶ Re: Risks of mail auto-reply ([RISKS-21.16](#))

Jerrold Leichter <jerrold.leichter@smarts.com>  
*Sun, 21 Jan 2001 15:38:18 -0500 (EST)*

In [RISKS-21.16](#), Dan Birchall writes about the exposure of  
possibly-sensitive  
data - where someone works, when they'll be away, who else works  
with them -  
in e-mail automatic responses.

The more things change, the more they stay the same. Seven or  
eight years  
ago, when some variant of the old "vacation" program - which  
implemented  
such messages on Unix systems - became widely used, there were a  
bunch of  
flames on the old Unix-Haters mailing list about the deluge of  
junk  
"vacation" messages sent mailing lists. I humorously suggested  
at the time  
that the appropriate way to get across the message that this  
wasn't the kind  
of thing everyone in the world wanted to - much less *\*should\** -  
see would be  
to create a new Usenet group, alt.houses.nobody-home, to which  
such messages  
could be gatewayed. For even greater effect, any readily  
available  
information (from phone books and such) could be added.

These days, of course, the Internet is \*much\* larger, and it's \*much\* easier to go from a name to an address and from an address to such information as how likely there are to be valuables in homes in the area.

It continues to astound me that people blindly let thousands of absolute strangers know not only that they will be away, but often for exactly how long - and often even where they will be. These same people probably are careful to have their mail picked up, their newspaper deliveries stopped, and lights on timers going off and on around their houses, all so that they don't look empty!

Jerry

---

## **⚡ Hotmail declines to accept new users with reserved words in last names**

"Robert Rossa" <rossa@csm.astate.edu>

*Thu, 25 Jan 2001 14:12:28 -0600*

For example, if your name is Billingsley, you get an error message when you try to sign up. The objectionable word seems to be "Billing". Removing one 'l' lets you sign up.

---

## **⚡ ACM1 Message for RISKS Subscribers**

Lillian Israel <israel@hq.acm.org>

*Fri, 26 Jan 2001 09:54:39 -0500*

ACM examines the future of information technology (IT) and the potential impact of IT on science and society at "ACM1: Beyond Cyberspace," a special Conference (March 12-14, 2001) and Exposition (March 10-13), held at the San Jose Convention Center. Register at: <http://www.acm.org/acm1>.

Speakers include: Steve Ballmer (Microsoft), David Baltimore (California Institute of Technology); Rodney A. Brooks (MIT AI Lab); Bill Buxton (Alias/Wavefront); Vint Cerf (WorldCom); Rita Colwell (NSF); Sylvia Earle (National Geographic Society); Shirley Ann Jackson (RPI); Dean Kamen (DEKA and FIRST); Alan Kay (Disney Imagineering); Ray Kurzweil (Kurzweil Technologies, Inc.); Marcia McNutt (Monterey Bay Aquarium Research Inst.); Martin Schuurmans (Philips Center for Industrial Technology); and Neil de Grasse Tyson (Hayden Planetarium), with Bob Metcalfe as Master of Ceremonies.

The FREE "hands-on" Exposition, a "field day for the mind," geared for families and kids, will showcase the latest R&D software & hardware from 70+ companies, universities, and research/educational institutions.

ACM1 also features a FREE Educators Day (March 10th) that will address broad educational initiatives and provide educators with proven strategies for engaging girls and minorities in technology-based education.

For ACM1 educational offerings: <http://www.acm.org/acm1/educators>.



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 21: Issue 23

**Tuesday 30 January 2001**

## Contents

- [Satellite strike blows away DirectTV pirates](#)  
[PGN](#)
- [Senators critical of videogame violence](#)  
[NewsScan](#)
- [Could someone die from spam/relay rape?](#)  
[Sanner](#)
- [Hackers hit U.S., U.K., Australian government sites](#)  
[Keith A Rhodes](#)
- [Risks of pharmacy computer systems](#)  
[Isaac Hollander](#)
- [Receipts for Voting Machines](#)  
[Douglas W. Jones](#)
- [Flight data recorder in your car's airbag](#)  
[David Collier-Brown](#)
- [Re: Aircraft had near-miss in Finland](#)  
[Michael Walsh](#)
- [Re: The Chinook Crash](#)  
[Simon Pickin](#)
- [Re: Organiser Bugs](#)  
[Tyler](#)

[Mike Cepek](#)

● [Re: Risks of owning a cute domain name](#)

[Terry Carroll](#)

● [Seeing Y2K bugs everywhere](#)

[Andrew Klossner](#)

● [Re: 54 weeks in a year?](#)

[Lawrence K. Chen](#)

[Nick Brown](#)

● [Re: UK Trials of GPS controlled car speeds](#)

[Derek Ziglar](#)

[Brian Clapper](#)

[Andres Zellweger](#)

[Harlan Rosenthal](#)

[Peter Houppermans](#)

● [Symposium on Requirements Engineering for Information Security](#)

[Gene Spafford](#)

● [Info on RISKS \(\[comp.risks\]\(#\)\)](#)

---

## ✶ **Satellite strike blows away DirectTV pirates**

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

*Sat, 27 Jan 2001 20:53:16 -0800 (PST)*

On 21 Jan 2001, DirectTV remotely disabled about 100,000 smart-card enabled set-top boxes that controlled illegal reception of their satellite TV. (Buried in the programming code was a message that read "GAME OVER" -- for those who perused the code.) About 9.5 million legitimate subscribers pay something like \$50/month for the hardware and \$22/month for the programming. DirectTV estimates this will save them over \$100 million/year. The pirated operations involved the iterative installation of bogus software that

enabled access despite each successive vendor change to the programming code. DirectTV believes that the counteraction disabled all of those bogus smartcards containing illegal software. DirectTV is part of Hughes Electronics. [Source: P.J. Huffstutter and Jon Healey, \*LA Times\*;  
PGN-ed (How long will it be until the next-iteration hack occurs?)]

---

## ✶ **Senators critical of videogame violence**

"NewsScan" <newsscan@newsscan.com>  
*Fri, 26 Jan 2001 08:21:59 -0700*

U.S. Senators Joseph Lieberman, Herb Kohl, and Sam Brownback plan to introduce legislation that will punish companies that market excessively violent video games to children. Kohl, a Wisconsin Democrat, said:  
"Practically everybody in the industry still markets inappropriate games to kids, practically every retailer regularly sells these games to kids, and practically all parents need to know more about the rating system." But Doug Lowenstein, president of the Interactive Digital Software Association, which represents video game makers, argues that such legislation could violate the First Amendment guarantees of freedom of speech and might simply make it more complicated for the video game industry to police itself.  
(AP/USA Today  
25 Jan 2001; NewsScan Daily, 26 Jan 2001)

<http://www.usatoday.com/life/cyber/tech/review/games/2001-01->

[25-violence.htm](#)

---

## ✂ Could someone die from spam/relay rape?

<Sanner@flashmail.com>

*Sun, 28 Jan 2001 10:25:59 -0500*

Consider the following two spam emails, one sent apparently from a Birmingham (bhm), Alabama BellSouth.net dial-up via a mail server at a hospital in Easton, PA and the other (picked off news.admin.net-abuse.email) sent from a Jacksonville dial-up of Coastalnet.com via the same mail server to British Columbia.

You'll notice that the first one spent 84 hours in the hospital mail server, from 4:30 P.M. Wednesday until 4:30 A.M. Sunday.

Now it is possible that someone was sending important medical data through that mail server. Some lab instruments these days even use email--I once received porno spam via what I was told was a microscope at a Belgian university. (the university hadn't known that the microscope was running sendmail and therefore hadn't bothered to take its usual precautions against spammers)

An 84-hour delay in important hospital email could, in theory, kill a patient.

By the way, I have noticed that these spams apparently for a pyramid scheme (International Global Prosperity?) come from all over the

country and use  
the same open mail server for mail sent in a certain week or so.  
Assuming  
that third party relaying of bulk email without explicit  
permission of the  
server owner is a crime, there appears to be an interstate  
criminal  
conspiracy.

---

## **⚡ Hackers hit U.S., U.K., Australian government sites**

"Keith A Rhodes" <RhodesK@GAO.GOV>

*Tue, 30 Jan 2001 07:43:16 -0500*

Attrition.org reports that hackers attacked government sites in  
the U.S.,  
U.K., and Australia last weekend, one of the "largest, most  
systematic"  
defacements of .gov/.mil sites worldwide. Check out  
<http://www.attrition.org/>  
for details. [Source: David Legard, IDG News Service, 22 Jan  
2001; PGN-ed]

---

## **⚡ Risks of pharmacy computer systems**

Isaac Hollander <ysh@mindspring.com>

*Fri, 26 Jan 2001 13:12:35 -0500*

I have patronized the same pharmacy for several years now.  
Today I went to  
fill a prescription (bad flu season this year)... A new  
pharmacist was  
behind the counter, so she meticulously checked my insurance  
information,

address, date-of-birth, and other pertinent data.

Initially, she refused to fill my prescription because my date-of-birth in her computer was in 1946. I was only able to convince her that my date-of-birth was in 1970 by reciting a list of all the prescriptions I've filled at this particular pharmacy, and by giving her my insurance card to prove that my policy information was correct.

The troubling thing is that I filled a prescription in the same pharmacy less than 1 month before. Something happened in the interim to corrupt my information -- an automated cleanup job, perhaps. The risk is that next time it won't be my antibiotic but it'll be someone's heart medication, and the pharmacist won't be as willing to listen to reason.

Isaac

---

## **✶ Receipts for Voting Machines**

"Douglas W. Jones" <jones@cs.uiowa.edu>  
*Mon, 29 Jan 2001 16:43:08 -0600 (CST)*

An article in *\*The New York Times\**, 28 Jan 2001, entitled "Nation Awash in Ideas for Changing Voting", included the following paragraph:

> Ideas include changing Election Day to a weekend or making it a  
> federal holiday, closing polls at the same time across the  
country,  
> allowing voter registration on Election Day and requiring that  
> machines give voters receipts.

Since the confusion surrounding the November election, I have heard several proposals that voting machines should give receipts. This is an extremely dangerous proposal!

If a voting machine gives a voter a receipt indicating the votes he or she has cast by, someone intent on buying a vote could demand to see that receipt as a condition of payment. Today, for example, unions can urge their membership to vote the union line, and employers can urge their employees to vote the company line, but they have no way of knowing if a particular member or employee followed their advice. Receipts would change this, opening the door to a class of election fraud that has not been widespread in the United States since the 19th century.

There are two ways to make voting machine receipts safe against this kind of fraud. One is to eliminate ballot content from the receipt, reducing it to mere proof that the voter has voted. This eliminates the value of the receipt as proof against the kinds of problems voters had in Florida last November.

The other approach is to issue the voter a receipt, but to deny the voter the right to take the receipt from the polling place, for example, by requiring that the voter deposit the receipt in a special box. If we do this, we may as well consider this box to be a ballot box, with the receipt being elevated to the official status of a ballot, and the voting machine, no matter how computerized, reduced in status to a ballot

marking device.

The official hand-recountable record of the vote then becomes the paper ballot issued by the machine.

Since the only votes that should be counted are those actually deposited in the ballot box, this second approach eliminates the need for the computerized voting machine to record any votes in its internal memory.

Optical mark reading of machine-printed ballots should be extremely easy, but for auditability, no information should be included on the machine-printed ballot other than human-readable content, and in fact, audits of the voting machine and ballot reading software would have to include checks to make sure that there is no use of steganography to include additional information on the paper ballot that might be used to connect it to a particular voter.

Douglas W. Jones, Assoc. Prof. of Computer Science, University of Iowa  
Chair, Iowa Board of Examiners for Voting Machines & Electronic Voting Systems

[Note that Rebecca Mercuri's PhD thesis (noted here previously) provides voter confirmation of a paper record, but that record is never handled by the voter:  
<http://www.notablessoftware.com/evote.html>  
PGN]

---

## **✈ Flight data recorder in your car's airbag**

David Collier-Brown <davecb@canada.sun.com>  
*Tue, 30 Jan 2001 08:22:24 -0500*

\*The Toronto Star\* (thestar.com, article by Paul Legall) reported on 25 Jan 2001 that the Ontario Provincial Police can now read the "event data recorder" units that are part of auto air-bags. The information includes speed (as you'd expect), but also braking, whether the driver's seat belt was fastened, if the ignition was turned on after the air bag went off and if there were other impacts before the one that set the airbag off. The speed information was disclosed to a coroner's jury recently.

David Collier-Brown, Performance & Engineering Team, Americas Customer Engineering 1-905-415-2849 davecb@canada.sun.com

---

## ✈ **Re: Aircraft had near-miss in Finland ([RISKS-21.22](#))**

Walsh Michael <michael.walsh@wmdata.fi>  
*Mon, 29 Jan 2001 12:49:39 +0200*

After I sent off my piece to RISKS, I noticed nothing more in the papers. However, on showing my wife the issue, she remarked that after that, they discovered that other planes not just Russian ones were disappearing from radar screens at Helsinki airport, and then traced the fault to probably being caused by building work at the airport.

It seems that once the Russians were out of the picture (pun, not intended, but noticed), the story became of less interest to the papers

here and so  
fell below my horizon (oops).

(As we're talking about building works here, maybe the Mickey Finn comment wasn't so far off !)

Mike Walsh, FIN-00300 Helsinki, Finland <michael.walsh@wmdata.fi>

---

## ✉ Re: The Chinook Crash ([RISKS-21.14](#),18-20,22)

Simon Pickin <Simon.Pickin@irisa.fr>

*Mon, 29 Jan 2001 18:47:29 +0100*

It certainly seems to be the case that important persons have more risk of being involved in serious air crashes than the rest of us mortals, particularly crashes coinciding with important political events in which they are involved, such as, just to pick one example, the start of serious peace negotiations between warring factions. In such cases, more "unconventional" explanations should not be completely ruled out and should perhaps even be voiced explicitly (at the risk of being called various sorts of names). An example of such a crash, in the press again recently on the occasion of its 20th anniversary, is the one killing the Portuguese prime minister Francisco Sa Carneiro and his defense minister Adelino Amaro da Costa on 4 Dec 1980. Time will (perhaps) tell. Just an observation.

Simon Pickin <simon.pickin@irisa.fr>

---

**⚡ Re: Organiser Bugs (Ladkin, [RISKS-21.21](#))**

<tyler@mango.net.nz>

*Sat, 27 Jan 2001 10:19:47 +1300*

Three Words: Disaster Recovery Trial

The simplest way of making sure your backups are working, is to try restoring them. We sit down and do this and document how to with all our clients servers yearly and whenever a big change is made on their servers. I find about 90% of the time on new clients servers, we couldn't restore the server/data on the first attempt due to various problems. Better to find out in a test run, than in a panic situation at 2AM on a Monday morning. (Or the middle of a trial.)

To extend a catchphrase, If your information is important enough to backup up, it's important enough to test restoring it.

Tyler Rosolowski

---

**⚡ Re: Organiser Bugs (Ladkin, [RISKS-21.21](#))**

Mike Cepek <mike.cepek@usa.net>

*26 Jan 2001 08:35:59 CST*

I also had to replace my well-worn and relied upon Palm III

after a catastrophic failure. There are two key differences in our experiences, however.

Firstly, I used the (also free) Palm Desktop product which came with the device from the manufacturer. The software works with Windows and Macintosh. (No flames please, I *\*do\** support freeware, shareware, Linux, etc).

Secondly, my restoration was quick, easy, and complete. At least I have yet to find any missing data (I do take your point: how can I really know it's *\*all\** there?). I trust that any such problems would be fixed by now in such a popular product, since lots of people besides me have needed to perform restores.

The risk I see here is assuming recompiled freeware would have the same quality that similar software from the manufacturer would have.

---

## **✉ Re: Risks of owning a cute domain name (Griffith, [RISKS-21.21](#))**

Terry Carroll <carroll@tjc.com>

*Fri, 26 Jan 2001 11:49:25 -0800 (PST)*

> As owner of the domain "dweeb.org" [...]

It doesn't have to even be "cute." I have tjc.com. Several times a week, I receive email intended for: the True Jesus Church (whose domain is tjc.org); a company in India named Tata Johnson Controls Automotive Ltd.

(whose domain is something like tjc.co.in, but who apparently took out an employment advertisement listing an email address of careers@tjc.com as the contact point); Piper Jaffrey Company, and investment company (pjc.com; about half of these email messages contain what should be highly confidential information; I enjoy copying all parties on my email message pointing out that they've sent this information out to a random recipient (and yes, I do then destroy the confidential email)); and, most maddeningly, students at Tyler Junior College in Texas (tjc.tyler.cc.tx.us).

The Tyler kids are most maddening, because they freely give out an erroneous tjc.com address to Web sites that harvest for spammers. The Piper Jaffrey case is the biggest Risk, though.

Interestingly, I haven't detected significant email that should be for the TJC Network (tjc.net); and the Piper Jaffrey case seems to be the only consistent off-by-one-letter error.

Terry Carroll, Santa Clara, CA <carroll@tjc.com>

[Various similar comments from others. PGN]

---

## ✶ Seeing Y2K bugs everywhere

Andrew Klossner <andrew@user2.teleport.com>

*Mon, 29 Jan 2001 08:23:14 -0800*

Ethan McKinney wrote that he received a \$0.00 bill in January for a canceled

credit card and opined that it was probably a Y2K bug at work.

I always receive a \$0.00 bill the January after I cancel a credit card. The January bill doubles as an end-of-year tax statement, showing the total amount of interest paid during the previous year.

Y2K gets far too much credit for perceived computer malfunctions.

Andrew Klossner (andrew@teleport.com)

---

## ✶ Re: 54 weeks in a year? (Dubery, [RISKS-21.19](#) and 20)

"Lawrence K. Chen" <lkc@cyberdude.com>

*Mon, 29 Jan 2001 22:15:52 -0500*

Just because a date is in a 'standard' format, doesn't mean it is meaningful to all.

Last year a VP of Product Development for a software company was traveling to Europe for a meeting. For entry to the particular country a valid VISA was required. Checking his old VISA he saw a date like '10/08/2000', and noted that October 8th, 2000 means his old VISA is still valid. Unfortunately arriving in the European country, he was refused entry...because his VISA had expired on August 10th, 2000.

Fortunately, after some deliberation he was able to fly to a country that didn't have a VISA requirement, and conduct his meeting over video....  
Though he could probably have done it by video without leaving the US.

On the flip side, I stood behind a gentleman trying to deposit a foreign check that suffered from a similar confusion in date format. The US bank wouldn't cash the check because it had been excessively post dated, rather than seeing that it had been issued during the early part of this year.

Since I grew up in Canada, date confusion was so annoying...that I was in the habit of using ISO date format. Which has the advantage of making sorting by date much easier (at least it did until Y2K, because to save space on the mainframe the first two digits were dropped for date keys). Unfortunately, the US post office wouldn't accept a form where I had used ISO date format.

[Old story in RISKS, but manifestations keep recurring, and after all

RISKS seems to be laden with recurrences of old stories about which no one was paying adequate attention. PGN]

---

## **✶ Re: 54 weeks in a year? (Dubery, [RISKS-21.21](#))**

BROWN Nick <Nick.BROWN@coe.int>

*Fri, 26 Jan 2001 10:17:06 +0100*

This is just one example of a huge major problem, caused in no small measure by the lack of any mandatory formal training for programmers. That in turn results from the huge demand for IT systems, the shortage of people who can

program (even badly), and the evolution of technology which means that any training programme "appears" to be obsolete after three years (especially if emphasis is put on learning APIs rather than learning about the real world, which is what happens when you go on software manufacturers' training courses).

As Lauren Ruth Weiner pointed out in her indispensable book "Digital Woes", you wouldn't hire a 24-year-old architect to design a stadium. But the experienced team of architects you did hire might well be using software built by a couple of 24-year-old programmers who had never experienced the consequences of any sort of structural failure.

This week we received a consultant's resume from a software house. It is 12 pages long and has a pretty colour background picture of a forest scene (itself a RISK; the e-mail was so big that initially it couldn't be delivered to a default-configuration mailbox). This consultant is 25 years old and has been out of college for three years; every two-week-long assignment has been written up as if she had been the lead developer of Multics. We won't be using her services (at \$US 800 per day) to maintain our PeopleSoft database. But somebody will.

Nick Brown, Strasbourg, France.

---

**🚀 Re: UK Trials of GPS controlled car speeds ([RISKS-21.22](#))**

"Derek Ziglar" <dziglar@yahoo.com>

Sat, 27 Jan 2001 11:43:10 -0500

> The tests, which prevented the car from topping 30mph, 40mph and other...

This will also surely resurrect problems that dates back to a much older and simpler technology--fixed speed governors on cars.

Back in the early 1970's, my father worked in the administrative offices of a large local utility company. At that time, the US imposed stricter speed limits to conserve fuel. Thinking the company could set a shining public example, they decided to install speed governors in the company's fleet of sedans.

That lasted only a short while as the number of automobile accidents \*increased\* within the fleet because of several significant unanticipated factors. One was that these speed-restricted cars were still having to interact on the road with non-restricted vehicles--leading to situations where the restricted vehicle was at a disadvantage on emergency maneuvers such as accelerating out of danger. The other was that the drivers were used to driving unrestricted cars, so occasionally made risky driving decisions momentarily forgetting the restrained capabilities of their company vehicle.

These risks exist in the basic premise of imposing blanket restrictions on vehicles with no provisions for exceptions based on the actual circumstances the driver is facing at any moment. Many such technologies

cannot be guaranteed to be sufficiently safe until \*everybody\* has it and is operating on equal terms. This new system adds a lot of complexity to merely apply different governor speeds based on the specific road rather than the fixed maximum vehicle speed imposed by the old automotive speed governors.

Imagine being on a long downhill expressway with several large heavy tractor-trailers bearing down on you at substantially above the speed limit your vehicle is restricted to? Imagine having a car following you at 50 mph when you cross into a 40 mph zone and your vehicle is \*forced\* to reduce speed. I hope the driver behind you is equally alert and attentive to the speed limit change!

What I fear from the people so vigorously pushing these technologies is that such safety risks that were long ago learned will be overlooked or glossed over. Somehow the new high-tech approach leads people away from realizing the basic concept is not new and the new solution fails to address or resolve concept flaws proven in prior low-tech implementations. Not to mention any new safety risks introduced by the newer implementation.

Sadly, these may not come to light until the first driving fatality or, as in the case of my father's employer, the statistics of the system in large scale use show an alarming trend.

Derek Ziglar, Atlanta, GA

**⚡ Re: UK Trials of GPS controlled car speeds (Loughran, [RISKS-21.22](#))**

Brian Clapper <bmc@WillsCreek.com>

*Sat, 27 Jan 2001 13:10:36 -0500*

Aside from the obvious "will it work reliably?" questions, I wonder exactly what affect this will have on automobile accidents. Certainly there's a correlation between excessive speed and auto accidents, so one would naturally expect the number of auto accidents to decrease in response to technologically enforced maximum speeds. But there are also times when exceeding the maximum speed can prevent an accident. How many of us have found ourselves in a situation where it was necessary to step on the accelerator, not the brake, to avoid a hazardous situation? I know I have.

This approach to limiting excessive speeding seems as though it might throw the baby out with the bathwater.

Brian Clapper, bmc@WillsCreek.com

---

**⚡ Re: UK Trials of GPS controlled car speeds ([RISKS-21.22](#))**

Andres Zellweger <ZellwegA@cts.db.erau.edu>

*Mon, 29 Jan 2001 07:50:19 -0500*

We can only hope that the designers of the system for GPS control of automobile speeds being tested in the U.K. ([RISKS 21.22](#)) learn about inherent risks of such devices from the aviation industry's experience with envelope protection systems for aircraft control.

(I can just see myself trying to accelerate to avoid an accident ...)

Dres Zellweger, Embry-Riddle Aeronautical University

---

## ✶ Re: UK Trials of GPS controlled car speeds ([RISKS-21.22](#))

<H.Rosenthal@Dialogic.com>

*Fri, 19 Jan 2001 20:33:33 -0800*

The tests, which prevented the car from topping 30mph, 40mph and other limits, were "highly reliable" ...

How about: I have just enough time on a small road to pass this stopped delivery truck . . . oops, have to gas it a little to get clear of the oncoming traffic - but I can't! The speed limiter cuts in! To avoid speeding, let's have a head-on collision. How about something in the roadway, or flashing lights just as you cross rail tracks, or emergency vehicles nearby, or any other environmental factor that might make a moment of excess speed the appropriate and safer response?

And how quickly does it respond? How much of a delay is there between

speeding up and the system deciding that you shouldn't be allowed to go that fast? And do you - and the person behind you! - get warning that you're about to be slowed down?

Harlan Rosenthal

---

## ✦ **Re: UK Trials of GPS controlled car speeds ([RISKS-21.22](#))**

Peter Houppermans <Peter.Houppermans@paconsulting.com>

*Mon, 29 Jan 2001 17:09:24 -0000*

Just imagine how much fun you'll be having overtaking someone who's doing 29 miles in a 30 mile zone - overtaking being occasionally necessary but universally recognised as one of the most dangerous manoeuvres. Interesting idea - it actually removes a safety margin as you cannot speed up to make that manoeuvre as short as possible.

I also note how this cunningly avoids taking care of the root problem: driver education. It's easier to fix the car than the driver - so I'm eagerly awaiting the next experiment: cars with breathalysers...

---

## ✦ **Symposium on Requirements Engineering for Information Security**

Gene Spafford <spaf@cerias.purdue.edu>

*Sun, 28 Jan 2001 10:33:24 -0500*

Advance Program and Call for Participation  
First Symposium on Requirements Engineering for Information  
Security

5-6 March 2001. Indianapolis

Sponsored by Purdue University CERIAS, in cooperation with  
NCSU eCommerce Program, NIST, NIAP, ACM SIGSOFT, ACM SIGSAC

<http://www.cerias.purdue.edu/SREIS.html>

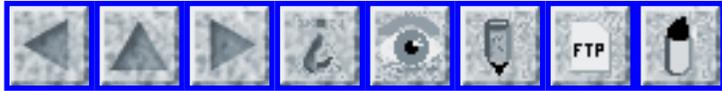
Security requirements for new electronic commerce and Internet applications exceed the traditional requirements for network security and traditional software systems. Security requirements are more complex and increasingly critical. Informally stated and de facto requirements are often of critical importance in the design and operation of these systems, but they are frequently not taken into account.

The symposium is intended to provide researchers and practitioners from various disciplines with a highly interactive forum to discuss security and privacy-related requirements. Specifically, we encourage those in the fields of requirements engineering, software engineering, information systems, information and network security, as well as trusted systems to present their approaches to analyzing, specifying, and testing requirements to increase the level of security provided to users interacting with pervasive commerce, research, and government systems.

The symposium will begin with short tutorials, include an invited keynote address by John Rushby of SRI, and include talks, breakouts, and a panel session. The symposium will be followed by a National Summit sponsored by

NIAP to bring together parties from government, industry, and academia to talk about how to design better software.

A preliminary program, tutorial information and registration information are all available online at the symposium WWW site: <<http://www.cerias.purdue.edu/SREIS.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 21: Issue 24**

**Thursday 15 February 2001**

## Contents

- [Calligraphy, computers, and Chinese culture](#)  
[NewsScan](#)
- [Lost pet fees cost Toronto \\$700,000](#)  
[Perry Bowker](#)
- [Network Solutions Sells Out -- Domain Info For Sale to Marketers](#)  
[Lauren Weinstein](#)
- [Hacker defends his vandalism, blames the victims](#)  
[NewsScan](#)
- [AnnaKournikova worm](#)  
[rcooper](#)
- [It's the wolf! It's the wolf!](#)  
[David G. Bell](#)
- [Osprey crash involved "software fault"](#)  
[Peter B. Ladkin](#)
- [Privacy on New Zealand golf Web site](#)  
[Gavin Treadgold](#)
- [Risks of outsourcing: you can bank on it!](#)  
[Cris Pedregal Martin](#)
- [Microsoft Hotfix undoes previous good](#)  
[Graham Bell](#)

- [SiteGuest.com: Unauthorized e-mail address capture whilst browsing](#)  
[Stewart C. Russell](#)
  - [The very friendly skies of United?](#)  
[Steve Bellovin](#)
  - [Risks inside my Jan 2001 American Express bill](#)  
[Thomas Maufer](#)
  - [Domain name mismatch family feud](#)  
[James Ryan](#)
  - [RISKS of anticipating computer problems](#)  
[Eric Nickell](#)
  - [Satellite strike blows away DirectTV pirates](#)  
[Serguei Patchkovskii](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

## ✂ Calligraphy, computers, and Chinese culture

"NewsScan" <newsscan@newsscan.com>

*Thu, 01 Feb 2001 09:42:58 -0700*

A current debate among Chinese speakers revolves around anecdotal evidence that computer word processing is eroding the ability of people to write traditional characters by hand -- and thus constituting an attack on Chinese culture. But the same debate occurred a century ago, when the pen began replacing the calligraphy brush, which is now used by a tiny segment of the population and treated as an instrument of artistic expression rather than normal communication. Professor Ping Xu of Baruch College predicts that the computer will replace the pen, just as the pen replaced the brush: "Why would you still spend so much time on handwriting Chinese characters when

you are eventually going to use computers? In spite of the opposition against the pen, why did the pen prevail? Because the pen is much easier to use and much easier to carry around. If the computer can provide an easier way of learning Chinese characters and all the Chinese language skills, eventually it will prevail." (\*The New York Times\*, 1 Feb 2001 <http://partners.nytimes.com/2001/02/01/technology/01LOST.html>; NewsScan Daily, 1 February 2001)

---

## ✶ Lost pet fees cost Toronto \$700,000

Perry Bowker <[pbowker@attglobal.net](mailto:pbowker@attglobal.net)>  
*Thu, 15 Feb 2001 14:15:44 -0500*

... the city lost out on nearly \$700,000 in pet fees last year because

nearly half of Toronto's dog and cat owners were never billed. The staffer

who knew how to run the computerized billing system was laid off. [...]

only one city employee ever understood the system well enough to debug it

when problems arose. That person was lost last year [due to downsizing]

leaving no one to get things going again when the system ran into trouble

and collapsed. [Source: \*Toronto Globe and Mail\*, 15 Feb 2001]

The risks here are obvious, but the Y2K experience has shown that many

organizations are still lucky to have even one person who understands some

of their systems. There were lots of war stories about places where

applications were run religiously because no one knew what they

did, or why,  
or how - except they seemed to produce something or feed into  
something else  
- much less assess and correct any Y2K risk.

Perry Bowker

---

## **✦ Network Solutions Sells Out -- Domain Info For Sale to Marketers**

Lauren Weinstein <privacy@vortex.com>  
*Wed, 14 Feb 2001 19:59:31 -0800 (PST)*

See PRIVACY Forum Digest V10 #03 for the entire item:  
<http://www.vortex.com/privacy/priv.10.03>

---

## **✦ Hacker defends his vandalism, blames the victims**

"NewsScan" <newsscan@newsscan.com>  
*Wed, 14 Feb 2001 08:53:55 -0700*

Defending his vandalism as an attempt to do good, a 20-year-old Dutch student arrested for creating the so-called Anna Kournikova computer virus that jammed Internet traffic throughout the world justified his action by saying he "never wanted to harm the people" whose computers he infected. He claims he intended only to issue them a warning to tighten their Internet security, and insisted that "after all it's their own fault they got infected." (AP/\*The New York Times\*, 14 Feb 2001; NewsScan

Daily, 14 Feb 2001

<http://partners.nytimes.com/aponline/technology/AP-Tennis-Virus.html>;

as usual, copyright material, reprinted in RISKS with permission)

---

## **AnnaKournikova worm**

rcooper <rcooper@jamesconeyisland.com>

*Wed, 14 Feb 2001 09:34:20 -0600*

(from Esa-1, via Mark Luntzel)

Well, we have survived the AnnaKournilova worm, but unfortunately this worm is directly responsible for our fax machine blowing up. Apparently numerous employees at our company is in our Attorney's address book. Apparently the law firm got hit pretty hard. Funny thing is, instead it being emailed to the recepients they were faxed. Got a pile of about 250 pages where the worm itself was faxed to numerous people at our office. The fax machine just couldn't handle it and blew up. Being we thought this was quite funny, I wanted to share it with the list. John, we need a sanitizer for fax machines now :-)

---

## **It's the wolf! It's the wolf!**

"David G. Bell" <dbell@zhochaka.demon.co.uk>

*Wed, 31 Jan 2001 21:23:14 +0000 (GMT)*

It is now commonplace for commercial sites to operate through several different versions of the same name, often by the use of different TLDs. In some cases, this may be cause of the distinct function of certain parts of their system, as with the recommended use of the .net TLD. In other cases, it is an attempt to make it easy for customers, and harder for competitors.

After rather more than half a year of Real Soon Now promises, a new agricultural web site has opened for business, under the name of Globalfarmers. And they have as their main domain globalfarmers.com while also running globalfarmers.co.uk, as they are based in Scotland.

Naturally, they have a system of registration and logins and SSL. However, if you connect by the www.globalfarmers.co.uk address, the Verisign certificate presented in the establishment of the secure connection is for www.globalfarmers.com, which triggers a spate of warning messages.

Combine that with the 40-bit encryption, and I'm just paranoid enough to give up on trying to register.

I know of other sites with multiple names, and secure connections, and this is the first time I've ever seen the wrong certificate presented. Globalfarmers seem to have made some mistakes, but I'm also wondering just what it all means. The error messages are rather uninformative. There seems to be an assumption that I already know about how these security systems work. Meanwhile, the naive user is always being told to check the

padlock symbol displayed by the browser, and not how to respond to such error messages.

There's a whole slew of risks here, including the problem of false positives (aka crying wolf), and what such things do to the reputation of a dot-com.

David G. Bell -- Farmer, SF Fan, Filker, and Punslinger.

---

## **✈ Osprey crash involved "software fault"**

"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>

*Fri, 02 Feb 2001 21:27:21 +0100*

The investigation into the V-22 Osprey tilt-rotor crash on 11 Dec 2000 on approach to New River, North Carolina, about 7 miles away from the airfield, is almost completed. Lt. Gen. Fred McCorkle, who oversees Marine aviation, said the causes were a combination of hydraulics and software failure.

The V-22 has two engines, one at each end of its wing, turning large propellers that are much larger than normal propellers but much smaller than helicopter rotors. It has a helicopter mode for landing and takeoff, in which the engine nacelles are vertical and the rotors operate in "helicopter mode", and for cruise flight, the nacelles rotate horizontally so that the rotors operate as giant propellers.

The aircraft has recently completed its operational evaluation. During the

evaluation, one aircraft crashed in Arizona on approach to landing, killing 19 marines. This was put down to "vortex ring state" or "power settling" of one of the two rotors, a condition in which a descending helicopter rotor encounters its own downwash and is unable to produce required lift. This happened with just one of the two rotors of the aircraft, which flipped inverted since the other rotor was still producing adequate lift, and there was no altitude available to recover.

The opeval was not question-free, and some irregularities in maintenance records have recently come to light and are being investigated. The latest crash is believed to be unconnected to any maintenance irregularities.

Helicopters have two means of controlling the pitch of the rotor blades, that govern the movement of the aircraft, called collective and cyclic pitch. They also have a power control, and these three together form the flight control system of a helicopter. Collective and cyclic pitch controls on the Osprey are hydraulic, as on most helicopters, as is the system controlling the angle of the engine nacelles (and thus transition between forward and "helicopter" flight positions). The No. 1 hydraulic system failed on the Osprey at the moment the pilot started converting from forward-flight to helicopter mode. The nacelles had covered 10% of their travel, and the pilot immediately commanded the rotors back to forward mode. The aircraft crashed anyhow.

Here is how Aviation Week's Robert Wall described what then happened

(Aviation Week, "V-22 Support Fades Amid Accidents, Accusations, Probes", pp28-9, Aviation Week and Space Technology, January 29, 2001).

"The V-22 is equipped with a triple-redundant hydraulic system and a mechanism that is supposed to be able to compensate for hydraulics problems in on line within 0.3 sec. Hydraulic levels are monitored by the flight control computers that monitor system pressure, reservoir fluid levels and changes in those levels. If an anomaly is detected, a combination of local switching isolation valve [sic] and remote switching valve are supposed to reroute hydraulics fluid from other systems, in this case the second and third, to compensate for the loss in the primary system. But that emergency system failed because of a software problem [...]" Apparently, the Marines are not yet giving out details of the software problem.

It is worth noting that the V-22 hydraulics was designed to operate at 5,000 psi instead of the "normal" 2,000-3,000 psi, because it allowed use of smaller and lighter components. But it was the single largest failure item during 804.5 hours of operational testing.

It is important to note, as the Marines have pointed out, that the reliability of the hydraulics systems themselves have nothing fundamental to do with the tiltrotor technology, but were simply a design choice. It is important also to note that the "software problem" occurred in the operation of a failure-mitigation mechanism, which is only activated

during failure of a primary aircraft system. The original failure appears to have been purely mechanical. But it is well-known that it is difficult to assure the reliable functioning of systems that are activated only during rare failures.

Another report appears in Flight International, 20 January-5 February, 2001, p24, "USMC fights for Osprey's future", by Paul Lewis.

Peter Ladkin

[Also noted by Mike Beims, who added that the risks of an incompletely tested backup system are a recurring theme in this forum. PGN]  
[A subsequent article by James Dao appeared in \*The New York Times\*, 13 Feb 2001, and quotes the Marine Corps on the forthcoming report. PGN]

---

## **✶ Privacy on New Zealand golf Web site**

"Gavin Treadgold" <gav@rediguana.co.nz>  
*Wed, 31 Jan 2001 14:47:30 +1300*

Recently the New Zealand Golf Association moved over to a newer and some would say fairer handicapping system. One feature of this system is the handicapping web site ( <http://www.golf.co.nz> ). This site is currently down for maintainence.

On this site, golf club handicappers can enter golf scores for members,

which are then consolidated into a national database. On this site you can log in and review your most recent rounds (date and location are given). You can also search for any other golfer in New Zealand and view their history.

Cards are generally visible on the site within 2-3 days of the card being handed in.

This site has a lot of benefits for golfers in New Zealand.

1. Being able to monitor people you play with to ensure they are handing good cards in and are not 'farming' their handicaps.

2. Ensuring that out of town visitors to tournaments supply their correct handicaps.

3. Providing club, regional, and national rankings of golfers.

There are however a few recently discovered risks - hence the site being taken down and redeveloped.

1. Every user's login id consists of a three-digit club code, ie mine is 371 - Russley Golf Club, and a four-digit club member id. This gives every registered golfer in New Zealand a unique seven digit identifying id. There was initially no password to login, hence someone could guess seven digit numbers, or collect them as the member numbers are printed out on the handicapping lists at the golf clubs. You are able to record your email address, and create a list of friends. This information could have been farmed by a spider/crawler. FIX? Use more than just a unique identifier that

is easily guessed.

2. A golfer's record displays recent rounds and their home course. The link can then be made between someone being on holiday and handing in out-of-town cards. Joe Smith lives in the South Island, but has been handing in cards in the North Island for a few days now. Hmm, I'll use the Telecom White Pages ( <http://www.whitepages.co.nz> ) to find his address and phone number... say no more. FIX? Delay the display of any out-of-region cards for x days.

3. And another goody related to the second point. Employers and employees can keep an eye on each other to see how much golf they are playing, and if they are calling in sick and then having a game of golf! Ha! I'll bet this is the real reason the site has been taken down - all the executives complained that their sub-ordinates could see how much golf they really were playing. FIX? Nah, this one is too much fun to take away :)

It will be interesting to see what sorts of fixes they have made once the site comes back online. Most people I have talked to about the site are supportive of it, with a couple of minor modifications to reduce some of the above risks.

=== Press Articles

Golf: Website pulled after privacy concerns

<http://www.stuff.co.nz/inl/index/0,1008,588486a1823,FF.html>

Golfers chipping back over page

<http://www.stuff.co.nz/inl/index/0,1008,593772a1601,FF.html>

I can see the sub-par PGN jokes now... :)

Gavin Treadgold, Red Iguana Ltd

---

## **✶ Risks of outsourcing: you can bank on it!**

Cris Pedregal Martin <cris@cs.umass.edu>

*Mon, 5 Feb 2001 12:47:50 -0500*

Summary: I left one bank because of their incompetence, and the new bank gave me an ATM card with my name and password, but linked to someone else's account. The RISK is embracing business models without regard to their technological implications, outsourcing in this case.

Banks are a well-established source of RISKS-lore, but my recent experiences are starting to convert me into a believer in the existence of RISKS-karma. After many hours spread over months of unpaid consulting to my formerly small regional bank, trying to get them to (a) refund the double debit for a safe rental and (b) record that I had paid at least once, so I could actually access my safe, I decided to take my business elsewhere, and opened an account in my local (still) small bank. It does not take a RISKS reader to do this cautiously, so I waited for new checks and the automatic deposit to switch over before trying to use my new account... my very first ATM operation was a balance request, which yielded an amount well below the expected. Went to the brick'n'mortar office, where a check of their computers showed the correct balance. Although I was relieved I

wouldn't  
have to fight to get my money back, I knew things were bad  
because there was  
obviously (at least) two different, not mirrored, databases at  
play here. I  
had to demonstrate the problem at their own ATM there, several  
times, before  
they'd start investigating, and after a good 30 minutes of  
consultations  
they admitted that yes, the card was linked to someone else's  
account, then  
had the gall to sternly ask me whether I had taken any money  
out, and then  
took another 20 minutes to "push through" the change, with some  
muted  
apology from the lowest-level employee involved.

Turns out that they outsource the printing of ATM cards, and  
they outsource  
the running of their ATM machines, presumably to two different  
companies,  
and evidently they move information from their own database to  
these other  
organizations... in a very RISKy manner.

The RISK here is familiar: embracing a business practice without  
understanding its technical underpinnings. The current  
management fads of  
outsourcing everything assume (implicitly!) well-defined and  
well-executed  
interfaces. In this sense, I am much luckier than PGN and other  
Californians  
who are experiencing a large scale version of the same with  
their supply (or  
lack thereof) of electricity.

Cris Pedregal Martin - Computer Science, UMass - <http://www.cs.umass.edu/~cris/>

---

## **Microsoft Hotfix undoes previous good**

<BELLG@allianz.com.au>

Thu, 1 Feb 2001 10:05:37 +1000

Good system administrators apply Hotfix packs to their systems promptly, to ensure known vulnerabilities are closed as soon as possible. Of course it is also wise to test the Hotfix to ensure it does not create new problems (and we all do that, of course). But who tests to see if it reintroduces problems/vulnerabilities removed by previous fixes?

It looks like we all should start full security regression testing of Hotfix packs, following the release of the recent Microsoft Security Bulletin MS01-005 , which includes the following statement:

"An error in the production of the catalog files for English language

Windows 2000 Post Service Pack 1 hotfixes made available through December

18, 2000 could, under very unlikely circumstances, cause Windows File

Protection to remove a valid hotfix from a system. The removal of a hotfix

could cause a customer's system to revert to a version of a Windows 2000

module that contained a security vulnerability."

Graham Bell, Allianz Australia

---

## **SiteGuest.com: Unauthorized e-mail address capture whilst browsing**

"Stewart C. Russell" <stewart@ref.collins.co.uk>

*Tue, 13 Feb 2001 11:27:15 +0000*

I was looking at an estate agent's (realtor's) website when I noticed the status line on my browser saying "Contacting <mailserver>" then "Message Sent". I looked through the site's HTML code and there was a little piece of JavaScript which appeared to send an e-mail message to the site's owner with no intervention from me. This service is provided by <http://www.siteguest.com/>, who describe it as "Caller ID for your web site".

Sure enough, in the next few days I started to get a number of e-mails from this realtor promising the best deals on houses. I'd prefer to choose who gets my e-mail address, and the behaviour of this particular individual has pretty much guaranteed no business from me.

The risk? The usual JavaScript and security warnings should be on, and that combining web and mail functions in one program is not always a good idea.

Stewart C. Russell Senior Analyst, Dictionary Division,  
HarperCollins  
Publishers, Glasgow, Scotland [stewart@ref.collins.co.uk](mailto:stewart@ref.collins.co.uk)

---

## The very friendly skies of United?

Steve Bellovin <smb@research.att.com>

*Thu, 15 Feb 2001 09:30:51 -0500*

According to the \*Wall Street Journal\*, 15 Feb 2001, the United Airlines Web site had a problem a few weeks ago: it was quoting preposterously low fares. For about an hour, some international fares were "zeroed out", and customers were being quote a price that included only taxes and fees. United is declining to honor the tickets purchased during this time, saying that customers should have known that a price of less than \$30 for a round trip from San Francisco to Paris wasn't reasonable.

Steve Bellovin, <http://www.research.att.com/~smb>

---

## **⚡ Risks inside my Jan 2001 American Express bill**

Thomas Maufer <tmaufer@acm.org>

*Thu, 1 Feb 2001 01:34:22 -0800*

The items on my American Express Bill are listed in chronological order, oldest first.

Beginning with items dated 1/1/2001, items dated from the future began to appear. For instance, the next several items were dated 1-Feb-2001, 1-Apr-2001, 1-Jun-2001, 1-Aug-2001, and 1-Sep-2001. It seems that they must have started interpreting the date as the month, and vice versa. The actual dates on the receipts corresponding to those items were 2-Jan-2001, 4-Jan-2001, 6-Jan-2001, 8-Jan-2001, and 9-Jan-2001.

I understand the mistake that they made (but I can't fathom the

reason that  
dates were corrupted), but I'm wondering what they'd say if I  
insisted that  
those charges be deferred until I actually \*make\* them, as I  
haven't  
actually made them yet.

Thomas Maufer

---

## 🔥 Domain name mismatch family feud

<James.Ryan@telemedianetworks.com>

*Wed, 31 Jan 2001 15:46:36 +1300*

A humorous story on similar domain names...

I own "yourmailinglist.com" and was recently afforded front-row  
seats to a  
family feud of mind-boggling proportions. It seems someone with  
a large  
extended family had sent out a personal newsletter updating all  
his  
relatives on his current state of affairs, the kids are fine,  
Mary's in  
College, Joe has a new job, etc. etc. Well, one of the  
recipients took  
great offence to receiving such an impersonal form of  
communications. He  
blasted the entire list with a scathing sarcastic attack on the  
original  
sender who he accused of "spamming" his relatives instead of  
sending each  
one a personal update.

In order to make himself "anonymous" he changed his reply-to  
address to  
"someone@yourmailinglist.com". Practically everyone on the list  
came back  
with their own scathing responses about how they were quite

happy to receive  
the newsletter about Mike and his kids, and shouldn't he be  
ashamed of  
himself for his insensitivity, etc. Of course, all these  
replies ended up  
in my mailbox...

I got my revenge, though. I simply "educated" all of those  
irate relatives  
in how to read an e-mail header, and soon they were blasting  
"Mr. Anonymous"  
at his proper address. The risk? If you're crazy enough to  
insult your  
whole extended family, be smart enough to know how to really  
cover your  
tracks...

---

## **✶ RISKS of anticipating computer problems**

Eric Nickell <nickell@parc.xerox.com>  
*Thu, 8 Feb 2001 10:48:47 PST*

My credit union, Xerox Federal Credit Union recently changed its  
website.  
In the process, I lost access to my account information via the  
web for 2  
weeks, somewhat troublesome since I have items that are charged  
to the  
account automatically and I've come to rely on web access to be  
able to view  
and transfer money between savings and checking to cover those  
charges. The  
changeover has been a comedy of errors, but in the end, customer  
service  
informs me that the problems were entirely my fault. Hmph.

First change I noticed was that I could no longer type in my 7-  
digit

PIN. I had originally been issued a 4-digit PIN, but feeling that this was insecure, I changed it. My estimates are that since XFCU gives 3 tries to get the PIN right, limiting the PIN to 4 numeric digits gives them a .3% chance of guessing the right PIN, given an account number. With a customer base of 70,000 members and account numbers of only six digits, how long do you think it would take a hacker to break into, oh,  $.3\% * 70,000 = 210$  accounts, eh?

In trying to get into my account with the 7-digit PIN, I used up my 3 tries. A customer service rep re-opened the account, but this led me to a debug page, so I assumed that I still didn't have the right PIN. Had to end up having the PIN mailed to my home address.

One week later, the mailed PIN arrived, I can see that it's a truncated form of my old 7-digit PIN, and we try again. Now, we land in a barf page. It's the sort of message a programmer puts up to flag system errors.

From the XFCU home, I click on the "contact" link to send them email. (It's right next to their "Most Useful Credit Union Web Site" award icon. How ironic.) The email comes back 24 hours later due to delivery problems. (The customer assures me that they have received no email complaining about this problem.)

When I call customer service, they're able to track down the problem in a few hours. Turns out in my correspondence with XFCU, they have always listed my account as "0369045" (not the actual number). I have always

fastidiously  
typed in the leading zero. Why? The reason I typed in the  
leading zero was  
a defense against the possibility that some stupid computer  
programmer would  
not treat "0369045" and "369045" and that believing the one  
received or  
printed communication was to be preferred. I was both right and  
wrong.

So, in the end, it was all my fault. Customer service informs me  
that they  
did not need to notify of the PIN change, because they initially  
issued  
4-digit PINS, and though the previous web access let members  
change to a  
longer PIN, THEY HAD NEVER given us permission to use a longer  
PIN.  
Further, I was the one at fault for typing in the leading zero.  
How stupid  
of me.

The RISKS here are obvious: Besides grumps about lowered  
security and  
truncating my PIN without bothering to inform me, there are two:

- \* The RISK of causing a breakdown in service by anticipating one.
- \* Second, a more traditional RISK: Knowing that there was one  
problem in the  
changeover (the truncated PIN), I lost sight of the fact that  
there might  
have been two (that I no longer allowed to type in the leading  
zero).

Eric Nickell, Xerox PARC

---

## **✶ Satellite strike blows away DirectTV pirates**

Serguei Patchkovskii <patchkov@ucalgary.ca>

Tue, 30 Jan 2001 17:07:53 -0700

: PGN-ed (How long will it be until the next-iteration hack occurs?)]

Not long at all. According to a very informative report in The Register (<http://www.theregister.co.uk/content/6/16377.html>), the DirectTV attack was directed at the old, and easily hacked, "H"-type smartcards, which were discontinued in 1999. The currently shipped cards, "HU"-type, are apparently somewhat more difficult to hack - but hacked versions are nonetheless already available, and were not affected by the attack. Neither were emulation-based systems, where a PC with the appropriate hardware connector impersonates a hacked smart card. Given that, according to The Register's sources, such hacks are not illegal in Canada, it won't take a lot of time before the new hacked cards become widespread. In fact, the DirectTV stike may even provide the pirates with a healthy cash infusion from all those people seeking to replace their now-defunct H-type cards.

Serge.P



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 21: Issue 25**

**Weds 21 February 2001**

## Contents

- [Millennium bug in travel agent system](#)  
[Debora Weber-Wulff](#)
- [Again: German government plans extensive surveillance](#)  
[Stefan Kelm](#)
- [Are free ISPs free? Juno says users must donate processor time](#)  
[Lenny Foner](#)
- [The old ones are the best ones: Hidden info in MS Word documents](#)  
[Paul Henry](#)
- [Modem misdialing seemingly at random](#)  
[Chiaki Ishikawa](#)
- [On paper-size standards](#)  
[Andrew Klossner](#)
- [More on the Friendly Skies of United](#)  
[Steve Bellovin](#)
- [Re: Risks inside my Jan 2001 American Express Bill](#)  
[Paul Green](#)
- [Re: SiteGuest unauthorized address capture](#)  
[Jean-Jacques Quisquater](#)
- [Re: Organiser Bugs](#)  
[Dennis Parslow](#)

[Peter B. Ladkin](#)

● [Re: It's the wolf! It's the wolf!](#)

[Martin Jost](#)

[Andrew Jackson](#)

● [When will they EVER learn?](#)

[Geoff Kuenning](#)

● [REVIEW: "Building Internet Firewalls", Zwicky/Cooper](#)

[Rob Slade](#)

● [Info on RISKS \(comp.risks\)](#)

---

## ✶ Millennium Bug in Travel Agent System

Debora Weber-Wulff <weberwu@tfh-berlin.de>

*Wed, 21 Feb 2001 08:18:04 +0100*

A friend with a travel agency sent me an article about the German Travel Reservation System Merlin. It seems that all the reservations made through the system were not credited to the January 2001 account, but to the January 2000 account. The problem was that Merlin was sending data to a back office system from Bewotec. Merlin, however, had not managed to change the year from 00 to 01. A speaker remarked: We didn't know that someone else was using the data too [for statistical purposes], but it is not a real problem, as no other cooperating systems have reported problems [!!!!] "Only" 200 travel agencies are affected, the ones that use Bewotecs Jack and Merlin from DCS.

Gee, that makes me feel better, then, if no one else has complained ...

Prof.Dr. Debora Weber-Wulff, Techn. Fachhochschule Berlin,  
Luxemburger Str. 10  
13353 Berlin, Germany weberwu@tfh-berlin.de <http://www.tfh-berlin.de/~weberwu/>

---

## ✂ Again: German government plans extensive surveillance

"Stefan Kelm" <kelm@secorvo.de>

Wed, 21 Feb 2001 09:47:49 +0100

Once again, plans by the German government to force ISPs to install surveillance interfaces for LEA access became known earlier this week. This is the third draft already, and a few things have changed.

Interestingly, the government itself (i.e., the Federal Ministry of Economics and Technology) has published the new drafts, which up to now are only available in German:

<http://www.bmwi.de/Homepage/Politikfelder/Telekommunikation%20%26%20Post/Telekommunikationspolitik/Sicherheit.jsp#TKÜV>  
[broken URL, and may not work anyway... PGN]

Stefan Kelm, Secorvo Security Consulting GmbH, Albert-Nestler-Strasse 9,  
D-76131 Karlsruhe +49 721 6105-461 kelm@secorvo.de, <http://www.secorvo.de>

---

## ✂ Are free ISPs free? Juno says users must donate processor time

Lenny Foner <foner@media.mit.edu>  
Fri, 2 Feb 2001 12:01:36 -0500 (EST)

See section 2.5 of <http://help.juno.com/privacy/agreement.html>

There are obvious privacy implications of being "volunteered" in this manner (hey, whaddya want for nothin'?). There are also obvious security implications, since Juno says absolutely nothing about what this distributed computation might be. ("Hi, we're Microsoft and we'd like to run a distributed computation that looks for duplicate copies of serial numbers in our products, and your user agreement says that we can format the disks of any machines that might possibly be infringing. Actually, we'd also like to format any disks that seem to have non-Microsoft operating systems installed.")

I'm also rather intrigued by their "we will run screensavers with ads and you're not allowed to turn off your machine." Seems to me that this will cost users -lots- of extra electricity if they're used to a screen saver that blanks the monitor and puts it in a low-power mode---and obviously the -computation- doesn't require the -screen- to be displaying anything; that's only the advertising function... And I'll bet there's some reasonable subset of users who don't know that they can turn off just the monitor, or don't realize that they're saving power when their screen blanks... With a "free" base of 14.5 million subscribers, and 100W/monitor (probably an underestimate), this is an entire nuke plant of extra load just

to keep  
those monitors from screensaving. I'll bet that's just -  
exactly- what  
California wants to be happening right now...

- - - Begin forwarded message - - -

Date: Fri, 02 Feb 2001 10:17:25 -0500  
>From: Declan McCullagh <declan@well.com>  
Subject: FC: Are free ISPs free? Juno says users must donate  
processor time

[As one science fiction writer would say, TANSTAAFL. This is  
merely the  
natural evolution of the market for "free" services, and is  
hardly  
objectionable. True, it raises some privacy and security  
questions, but  
nobody's forcing you to use Juno, and pay ISPs are hardly  
expensive. --Declan]

[http://www.cluebot.com/article.pl?sid=01/02/01/2249220&](http://www.cluebot.com/article.pl?sid=01/02/01/2249220&mode=thread)  
mode=thread

How Free Are Free ISPs?

posted by vergil on Thursday February 01, @05:06PM  
from the check-that-clickwrap dept.

Free ISPs have been especially hard hit by the current dot-  
com

downturn. Juno Online Services (recently smacked by a  
Temporary

Restraining Order involving a patent infringement scuffle  
with rival

NetZero) has developed a novel way of extracting megahertz  
-- and

potential megabucks -- from its subscriber base. According  
to a

2/1/2001 InternetNews article, Juno's "Virtual Supercomputer  
Network"

aims to replicate the success of SETI@home by pooling the  
processing

potential of its new subscribers and selling the combined

computational power. According to Juno's new service agreement, Juno's subscribers "agree" to let Juno download, upload and run software from their PCs, and may be required "to leave" their computers "on at all times." [...]

[Lenny later added the following note. PGN]

Actually, given that it -could- be the case that such a distributed computation might be set to initialize every machine at a particular time, I can just see it now when all those zillions of monitors come out of screen-save simultaneously:

"California power grid destabilized by Juno, news at 11..."

(Even an earthquake doesn't move mice all over the state...)

---

## **✶ The old ones are the best ones: Hidden info in MS Word documents**

"Paul Henry" <emmo@hotmail.com>  
*Fri, 16 Feb 2001 16:03:49 -0000*

OK, this is an old one (dating back to 1994 according to the RISKS archive), but it was new to me when I came across it recently, and thought people might be interested in a couple of real life scenarios:

I received an MS Word document from a software start-up regarding one of their clients. Throughout the document the client was referred to as "X", so

as not to disclose the name. However I do not own a copy of Word, and was reading it using Notepad of all things, and discovered at the end the name of the directory in which the document was stored -- and also the real name of the client!

I checked on a number of other word documents I had for hidden info, especially ones from Agencies who are looking to fill positions -- and yes, again I was able to tell who the client was from the hidden information in the documents.

Finally, I had a look at the Lockerbie Judgment document:

<http://www.scotcourts.gov.uk/html/lockerbie.htm>

Hoping to find something that would cause international uproar -- alas, no, just an ironic hidden message: "Are you surprised?". Yes, I was, actually -- I thought Ahmed Jibril did it.

Risks: What potentially damaging information is hidden in published documents in Word, PDF and other complex formats?

Mitigation: Use RTF when you can -- no hidden info, no viruses.

Paul Henry, emmo@hotmail.com

---

## ✶ Modem misdialing seemingly at random

Chiaki Ishikawa <Chiaki.Ishikawa@personal-media.co.jp>  
*Tue, 6 Feb 2001 20:28:13 +0900 (JST)*

Modem misdialing seemingly at random

RISKS has seen its share of mis-configured modem setup forced PCs calling somebody's house (in some cases police station?) unintentionally at random.

Here is a new twist from Japan.

Modem chips used in about 6 million PC units of 24 million PCs shipped in Japan after the summer of 1998 has shown a peculiar problem.

When the modem is asked to dial telephone line using so called "Pulse Dial" mode, it fails to properly dial the requested number, and instead calls wrong number (!) seeming at random under high load of the OS (Windows 98),

Pulse dialing (as opposed to tone dialing) is used in many Japanese telephone subscriber lines. How many users of the affected 6 million units use pulse dialing is anyone's guess: one educated guess puts the number at about 2 million users. This high concentration of the pulse dial telephone subscriber lines in Japan has caused quite a problem with the modem.

I noticed that a large Japanese ISP, @nifty, (URL: [www.nifty.com](http://www.nifty.com)) has been warning the user for quite some time by sending periodic warning and mentioning various manufacturers comments, whose PCs may or may not dial incorrectly sometimes. This happened since early last summer if I recall correctly.

\*Mainichi Shimbun\* newspaper Web site lately announced the

problem in its  
IT-related Web page and it mentions the following PC  
manufacturers whose  
products are affected: Fujitsu, NEC, Toshiba, Sony, Japan IBM,  
Hitachi, and  
Epson.

<http://www.mainichi.co.jp/digital/index.html> (in  
Japanese)

Gateway Japan was quoted as investigating the situation, and it  
seems that  
Apple didn't answer the inquiry from the newspaper yet.

The problematic symptoms occur under windows 98. It seems that  
the modem  
tries to use the software timing to produce proper number of  
pulses per  
seconds to generate correct dialing signals. However,  
obviously, Windows 98  
can't let the software driver have enough CPU time under high  
load, and the  
software timing becomes bogus, thus the wrong dial number.

Some people have receive these bogus calls many times and it  
seems that  
their tenacity uncovered the problem.

The modem chip in question is build by Conexant. Their Web site  
mentions  
that the drivers ought to be provided by their OEM customers,  
which makes  
sense. (Warning: before trying to access Conexant Web site, you  
might want  
to check out your browser's cookie setting. The Web site tries  
to set many  
cookies as if there would be no tomorrow. I had enabled  
"Warning before  
accepting cookies", and I had to kill my browser! I had to  
disable the  
warning to access the URL. My browser is Netscape. YMMV. )

Affected PC manufacturers have begun offering modified drivers

that add  
"dial number verification step"(?) according to Mainichi Web  
page. (From  
what I gathered by reading an attached file from IBM Web site,  
the driver  
checks the system load before dialing and if it expects that the  
load is too  
high to perform pulse dialing reliably, it aborts the dialing  
and hangs up.  
Various PC vendor sites mention that the cause of the high load  
is  
mentioned: CD drive, FDD, HDD, etc..)

Although the mis-dialing is reported to occur very rarely per  
modem, the  
problem seems grave enough and the affected PC vendors and one  
industry  
association obviously sends a joint press release to let the  
users become  
aware of the new modified drivers. If you have 2 million users  
trying to  
dial the access points of the ISPs, my guess is that the  
incorrectly dialed  
numbers tend to fall in a select few ranges and thus irate  
complaints.

Tone dialing users are not affected at all.

(I wonder if the same problem may be observed elsewhere where  
pulse dialing  
is used by a large user base and the same Conexant chips are  
widely  
used. The Mainich page left the impression that pulse dialing is  
not used  
widely anymore.)

Chiaki Ishikawa Personal Media Corp. Shinagawa, Tokyo, Japan 142-  
0051  
ishikawa@personal-media.co.jp.NoSpam

## ✶ On paper-size standards (Re: Kuhn, [RISKS-21.21](#))

Andrew Klossner <andrew@user2.teleport.com>

*Fri, 26 Jan 2001 10:58:37 -0800*

Markus Kuhn, in writing about ISO standards for numbering weeks, also makes mention of a reference to ISO paper sizes, which includes this statement:

"Conversion to A4 as the common business letter and document format in North America would not cause any significant cost."

This pronouncement considers only the cost of computing equipment such as printers. It ignores the substantial amount of non-computer infrastructure. As one example, my neighborhood elementary school has hundreds of three-ring binders and clipboards as well as non-metric paper trimmers, book binders, hole punchers, and ancient duplicating equipment. Anyone familiar with the state of U.S. public education understands that money to convert all this to metric paper sizes will not be available in the foreseeable future.

The RISK here concerns enthusiasm for elegant technical solutions which overlook the cost of abandoning current practice.

Other disparaging remarks, such as the "bizarre" way that we norteamericanos measure paper density, would perhaps be more compelling if they did not come from an island where everyone drives on the wrong side of the road.

Andrew Klossner (andrew@teleport.com)

## ✈ **More on the Friendly Skies of United ([RISKS-21.24](#))**

Steve Bellovin <[smb@research.att.com](mailto:smb@research.att.com)>

*Mon, 19 Feb 2001 22:38:23 -0500*

I just saw an update on CNN that says United Airlines has decided to honor the tickets [purchased on their Web site, e.g., for less than \$30 -- instead of \$300... PGN].

Steve Bellovin, <http://www.research.att.com/~smb>

---

## ✈ **Re: Risks inside my Jan 2001 American Express Bill**

Paul Green <[Paul.Green@stratus.com](mailto:Paul.Green@stratus.com)>

*Tue, 20 Feb 2001 10:00:33 -0500*

I can provide the likely answer to Thomas Maufer's question as to how the dates became corrupted on his American Express bill. First, I have no connection with American Express (other than as a long-time holder of several of their cards), so this is an educated guess. But I have been the Y2K coordinator for one of the Stratus Computer operating systems. We warned our customers in December 1999 that if they continued to use 2-digit years after January 1st, 2001, they might into the precise interpretation problem described in Thomas's letter. The details are specified at <ftp://ftp.stratus.com/pub/vos/doc/y2k/sray2k21.htm>. I have no

idea whether  
this error arose on one of our products, or on a different  
vendor's product.

When a date in the format MM DD YY is converted using a rule in  
the format  
YY MM DD you will get exactly the conversion noted in this  
report.

01-02-01 is interpreted as 2001-Feb-01 rather than Jan-02-2001.  
01-04-01 is interpreted as 2001-Apr-01 rather than Jan-04-2001.  
and so on.

Things will get interesting after January 12th; I wonder what  
Thomas's bill  
looks like for items charged on the 13th and beyond? Who would  
have thought  
that computers would be susceptible to triskaidekaphobia!

Paul Green, Stratus Computer, 111 Powdermill Road, Maynard, MA  
01754-3409  
Senior Technical Consultant TEL +1 (978) 461-7557 FAX +1 (978)  
461-3610

---

## **⚡ Re: SiteGuest unauthorized address capture (Russell, [RISKS-21.24](#))**

Quisquater <jjq@dice.ucl.ac.be>  
*Fri, 16 Feb 2001 10:56:27 +0100*

<http://www.privacyfoundation.org/advisories/advEmailWiretap.html>  
gives an exploit that allows the spying ("wiretap") of written  
messages and  
used addresses when forwarding privately a received message with  
embedded  
code ...

Jean-Jacques Quisquater

---

## ✂ Re: Organiser Bugs (Ladkin, [RISKS-21.21](#))

"Parslow, Dennis" <Dennis.Parslow@FMR.COM>

Wed, 21 Feb 2001 06:46:49 -0500

Peter Ladkin points out the difficulty in discovering and recovering from slow corruption of data. In fact, in some sense, the most dangerous computer viruses are the ones (thankfully relatively few) that simply flip characters, slowly and at random. One of the first of these did so in Excel Spreadsheets...where two characters being flipped can clearly have a huge impact further along in calculations.

This also calls into light the backup strategies being used. Many keep their regular backups for approximately a month, and may or may not keep a full backup for longer. But if the problem was two months ago, give or take, many places that even do keep monthly backups may not have the information available to them from the incrementals in between, and a lot changes in a month. But management of more tapes may not be practicable in a large environment either...

---

## ✂ Organiser Failures ([RISKS-21.18](#),19,21.23)

"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>

*Wed, 31 Jan 2001 08:26:21 +0100*

Unfortunately, it seems as if the good points about backup housekeeping made by Tyler Rosolowski and Mike Cepek ([RISKS-21.23](#)) miss the main point that I tried to convey.

My experience showed that devices can fail "live", with what I called a disgraceful degradation. I have no evidence of any misbehavior from the backup software (although this is not ruled out). The measures suggested by Rosolowski and Cepek are appropriate as protection against one-time catastrophic events. It is unclear to me how they would protect against my type of failure.

Although Rosolowski's point about making regular comparisons between new data and old data is well taken, he doesn't suggest any time interval at which the differences might have overcome my perceptual threshold for noticing problems. Indeed, it is hard to see how he could, for the general case.

Mike Cepek suggested there were two main differences between his case and mine, but omitted what I suggested is the crucial feature.

As measures against failure, the suggestions from both contributors fall into the category of "good housekeeping" (GH). There is a general problem with such methods. Car drivers know that, for each accident, there is at least one prophylactic measure that would have avoided that individual

accident; the problem is to devise one single measure that would avoid every accident.

For backups, this is a solved problem. Backups are an example of a dependable database. There are algorithms well-analysed in the literature to ensure such dependability (either perfectly, or to a known very high degree of reliability). The solution to all backup problems is to use such a procedure (implemented through humans, software, whatever). In contrast, the dependability of most GH procedures is anecdotal only. Provided that one assures conformance of the backup machine itself (which may well be administratively out of control of the PDA user, therefore of higher backup software), one could use verified backup software which implements the appropriate part of a demonstrably dependable algorithm.

Except there isn't any for PDAs. One has to wonder why not.

Peter Ladkin

---

## ✶ Re: It's the wolf! It's the wolf! (Bell, [RISKS-21.24](#))

Martin Jost <Martin.Jost@icn.siemens.de>

*Fri, 16 Feb 2001 15:45:23 +0100*

> [...] I know of other sites with multiple names, and secure connections,  
> and this is the first time I've ever seen the wrong certificate presented.

Why should they get it right, if (even (?)) HP fails at it ?  
Try <https://www.itrc.hp.com>  
(this is HPs IT Resource Center)

You start with a warning from Netscape:

```
-----  
Warning! You have requested an insecure document that was  
originally  
designated a secure  
document (the location has been redirected from a secure to an  
insecure document). The document  
and any information you send back could be observed by a third  
party  
while in transit.  
-----
```

(I had to read this slowly to get it the first time; now I  
routinely  
click the 'Ok'-Button (Risk !))

Clicking 'Ok' carried me to  
<http://home1.itrc.hp.com>

Clicking "Maintenance and Support" on this page got me on to  
<https://europe-support.external.hp.com>  
(Note: To get there, you will need an account)  
I usually check this URL and the 'lock' icon in netscape.

This time no warning. (Certificate belongs to  
[europe-support.external.hp.com](https://europe-support.external.hp.com); 40 Bit)

And I remember having seen problems in the past of the sort:  
Something like <https://europe-support.external2.hp.com> in  
Netscape, but  
<https://europe-support.external.hp.com> in certificate  
(Looks like load balancing to me)

Martin Jost

---

**⚡ Re: It's the wolf! It's the wolf!**

"Andrew Jackson" <amj@trustis.com>

*Sat, 17 Feb 2001 18:17:23 -0000*

I agree that there are ways to present a certificate so that it matches the Web site name used, which would reduce the chance of receiving less than helpful warning messages.

However, the site in question is capable of using 128 bit SSL encryption -

I would guess that the 40 bit problem (and therefore a risk) results from having an out of date browser as all the current ones are capable of 128 bit encryption - even on this side of the Atlantic.

On a related tack, what gets me annoyed is Webservers that won't let me submit a PKCS#10 certificate request without putting something in the "State" field :- ( "Frustrated" is never accepted, either.)

Andy amj@trustis.com

---

## **⚡ When will they EVER learn?**

Geoff Kuenning <geoff@cs.hmc.edu>

*Thu, 15 Feb 2001 23:00:40 -0800*

I just signed up with netflix.com, which among other things allows you to purchase DVD movies. Within two days, I received an e-mail that helpfully told me -- in cleartext -- the password that I had just set up for the account.

Since movies are moderately expensive, there are literally tens of thousands of titles available, and it's not unreasonable to order 2-3 copies of one title, this seems to put my account at a rather high risk of being abused by anyone with a sniffer. I immediately changed the password, and so far I haven't been told \*it\* in cleartext. But when will people figure out that there's not a lot of point in using SSL if you fling sensitive information around in unencrypted e-mail?

Geoff Kuenning    geoff@cs.hmc.edu    <http://www.cs.hmc.edu/~geoff/>

---

## ★ **REVIEW: "Building Internet Firewalls", Zwicky/Cooper**

"Rob Slade, doting grandpa of Ryan and Trevor" <rslade@sprint.ca>

*Mon, 19 Feb 2001 08:30:48 -0800*

BKBUINFI.RVW    20010105

"Building Internet Firewalls", Elizabeth D. Zwicky/Simon Cooper/D.

Brent Chapman, 2000, 1-56592-871-7, U\$44.95/C\$65.95

%A    Elizabeth Zwicky

%A    Simon Cooper

%A    D. Brent Chapman

%C    103 Morris Street, Suite A, Sebastopol, CA    95472

%D    2000

%G    1-56592-871-7

%I    O'Reilly & Associates, Inc.

%O    U\$44.95/C\$65.95 707-829-0515 fax: 707-829-0104 nuts@ora.com

%P    869 p.

%T    "Building Internet Firewalls, Second Edition"

Cheswick and Bellovin's "Firewalls and Internet Security" (cf. BKFRINSC.RVW) has been, and probably will continue to be, seen as the classic reference with the seriously technical crowd. Chapman and Zwicky, however, created the first reference for the more normal run of system administrators: those whose lives do not revolve around hacking the UNIX kernel. This expanded edition fulfills the same task, and maintains the same reasonable stance. It is refreshing, for example, to find a work that, even if it doesn't know much about viruses, admits that firewalls can do very little to protect against them.

There is now a more general and introductory part one, discussing the basic concepts before getting deeply into technical details. Three chapters look at a rationale for firewall usage, Internet services and requirements, and universal security strategies.

Part two (part one in the original edition) is an introduction to firewall technology and structure. It could easily stand as a separate book, itself, clearly explaining the operation of, and reasoning behind, functions that other firewall books merely mention. More, it is a very down-to-earth and practical guide to evaluating security needs and planning for security systems and practices. The writing is completely clear, and the explanations first-rate. Two chapters look at the packet structures of Internet protocols and basic firewall technologies. Chapter six, on firewall architectures, is a perfect introduction for the manager who, while

not having a technical background, must lead or administer a security project, and is followed by a short but useful outline for a design process.

The detailed chapter on packet filtering is the longest in the book, but there is also solid coverage of proxy systems and bastion hosts. The section concludes with valuable particulars of tools for securing UNIX (and Linux) and Windows (NT and 2000) systems.

Part three reviews various Internet services, the reasons for having them, risks associated with them, and details that can be used to secure them.

There is an introduction to the subject, and then coverage of intermediary protocols, the World Wide Web, e-mail and news, file and print transfer and sharing, remote access, and real time conferencing systems. Each chapter also deals with related issues and technologies, such as the various specific mail protocols and active content for Web pages. As well, the topics of naming and directory services, authentication, administrative services, and databases and games are examined. Two sample firewall configurations, using the previous material, close off the division.

Part four provides quick but decent guidance on general security issues.

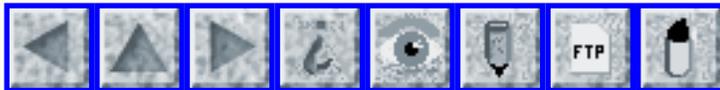
There is a look at security policies, firewall maintenance, and responding to security incidents.

The appendices are useful, outlining resources for further information, tools, and a brief but reliable explanation of cryptography. The resource

list, unlike the usual table of titles and URLs, contains quality works, and is annotated.

This was the first book to truly explain, to the non-specialist, the various factors and functions involved in firewall choice and construction. I still have not found another of similar quality. This new edition is not just an update, but a valuable extension and expansion. For those building their own and for those evaluating vendor proposals, this book is a must.

copyright Robert M. Slade, 1995, 2001    BKBUINFI.RVW    20010105  
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 21: Issue 26

Monday 5 March 2001

## Contents

- [Smart bombs miss again](#)  
[Lord Wodehouse](#)
- [Air gaps](#)  
[Bruce Schneier](#)
- [Bibliofind exposes lots of credit card data they shouldn't have had](#)  
[Lenny Foner](#)
- [TurboTax potential overstatement of gross income](#)  
[Richard Mason](#)
- [Risks of buggy cell phone networks](#)  
[Kragen](#)
- [SETI@Home felled by a Single Point of Failure](#)  
[Malcolm Pack](#)
- [Passwords don't protect Palm data, security firm warns](#)  
[Yves Bellefeuille](#)
- [Risks of laptop anti-theft devices](#)  
[Tony Yip](#)
- [Where does NAVSTAR say we are, again?](#)  
[James Paul](#)
- [Beware assumptions about keyboard layouts...](#)  
[Perry Pederson](#)

- [Re: On paper-size standards](#)  
[Gideon Sheps](#)
  - [REVIEW: "Tangled Web", Richard Power](#)  
[Rob Slade](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

## ✶ Smart bombs miss again

Lord Wodehouse <w0400@ggr.co.uk>

Thu, 22 Feb 2001 15:05:03 +0000 (GMT Standard Time)

>From BBC New online at

[http://news.bbc.co.uk/hi/english/world/middle\\_east/newsid\\_1184000/1184086.stm](http://news.bbc.co.uk/hi/english/world/middle_east/newsid_1184000/1184086.stm)

"Pentagon officials have admitted that most of the bombs dropped by US and British warplanes on Iraq last Friday missed their targets."

Yet again I find myself writing to RISKS to point out that these computer-game type weapons are almost always oversold on their abilities and have been little more effective than plain dumb bombs. The Patriot missile is another case oversold (see many article in RISKS).

However, if smart weapons fail in Iraq, how much less well will they work in Europe under bad weather. Kosovo was such a case and often the weapons could not be used. The military rely on them more and more, and yet they are shown to be more limited and often less usable.

Extending this on to the smart guns and systems for soldiers, I see the fighting forces becoming less effective. The small band of

fighters often  
now seem to beat the big armies. It will become worse, if  
technology is used  
exclusively.

And what about the NBMD system. Five failures so far. I do not  
see be being  
anything apart from a means of keeping some companies in work  
and something  
that destabilizes the current situation. Shooting down a long  
range missile  
is a lot harder than trying to hit a static target!

Global Research Information Systems, GlaxoSmithKline Medicines  
Research Centre  
Stevenage SG1 2NY UK +44 1628 482 634 w0400@ggr.co.uk [http://  
www.gsk.com/](http://www.gsk.com/)

---

## **✶ Air gaps**

Bruce Schneier <schneier@counterpane.com>  
*Wed, 21 Feb 2001 16:39:50 -0600*

This is from the February Crypto-Gram.  
<http://www.counterpane.com/crypto-gram-0102.html>

Whale Communications has been marketing something called e-Gap,  
which they  
claim is an "air gap" between two networks. Basically, the  
system consists  
of two servers. One is connected to the Internet and the other  
to the  
internal network. The two servers only connect through the e-Gap  
system, a  
SCSI-based memory device that gets toggled between them. The two  
servers  
are never directly connected.

This is an interesting idea, but it's not an air gap.

What E-Gap really does is create a proxy connection between two computers.

It's a slow connection. It's a very limited connection; the system strips down any network layers under the session layer. What that means is that if you set up a system using E-Gap and an intruder were to break into the Internet server, he could not obtain TCP/IP connectivity to the internal server. This certainly increases the security of the back-end server.

Nonetheless, the intruder can still access the back-end server as a regular client. The intruder can still break into the internal system by exploiting any vulnerabilities above the transport layer.

The whole point of an air gap is that there is no automated connection between the two devices. It's not simply that there is no physical connection between the devices most of the time, but that any logical connection between the two devices is not automated. If the Internet server and the back-end server were on opposite sides of a room, there would be an air gap between them. To connect the two computers, a user has to walk a floppy disk across the room. For an attacker to attack one computer from the other, he needs to be physically present. Even if an attacker gains access to the Internet server remotely, he cannot bridge the air gap to the back-end server.

While E-Gap can claim that with their device systems are "completely

disconnected at all times," the truth is that their switch operates automatically at all times. There is always a logical connection between the systems connected by their device. And that connection is subject to remote attack, and possible compromise.

I'm not saying that this is a bad product -- it sounds like a good product -- but it is not an air gap. Calling it one is deceptive marketing. Kind of like calling a stream cipher a one-time pad.

Whale's page describing their technology:

<[http://www.whale-com.com/fr\\_0300.htm](http://www.whale-com.com/fr_0300.htm)>

They call it "impenetrable." Also note that on their home page they don't just call it an air gap but a \*physical\* air gap, just in case someone might have wanted to give them the benefit of the doubt.

A response to critics by someone with Whale:

<<http://lists.gnac.net/firewalls/mhonarc/firewalls.199911/msg00269.html>>

Hall of shame puff piece:

<[http://www2.cio.com/archive/050100\\_development\\_content.html](http://www2.cio.com/archive/050100_development_content.html)>

Whale isn't the only one. Here's a review of six "air gap" products:

<<http://www.infosecuritymag.com/articles/july00/cover.shtml>>

Airgap Networks, which has few details on their product, is notable for actually defining "air gap" (albeit in an Orwellian manner).

<<http://www.airgap.net/what.html>>

Bruce Schneier, CTO, Counterpane Internet Security, Inc. 1-408-556-2401

3031 Tisch Way, 100 Plaza East, San Jose, CA 95128 <http://www.counterpane.com>

## ✂ Bibliofind exposes lots of credit card data they shouldn't have had

Lenny Foner <foner@media.mit.edu>

Mon, 5 Mar 2001 17:26:25 -0500 (EST)

Bibliofind matches up people looking for used books, and book dealers who have them. Every time you use it to actually buy a book, you're forced to enter all of your name, address, CC info, etc, etc, and that's then sent to the book dealer. They didn't appear to actually keep any of this information around, given that it was never presented in the UI (e.g., as a pre-filled-in form, or something else useful).

So I'm especially appalled to have just read that my data, along with about 100K others' data, was perhaps being read for the last 4 months.

See <http://www.cnn.com/2001/TECH/internet/03/05/bibliofind/index.html>

Not only did they -not- say they were keeping it (instead of just serving as a conduit), keeping it did nothing to make their customers'

lives easier. So it looks like they got it wrong coming and going.

Perhaps the press report got it wrong, and it was some sniffer-like

attack instead, but it sure seems to imply that they had a big database hanging around that they didn't tell their customers about

and which wasn't helping anybody, except to serve as a big fat target.

Feh. I guess we'll see if phantom charges appear on various cards.

Not to mention perhaps enabling identity frauds of various sorts.

I can't get any info about this directly from Bibliofind at the moment, because their site is off the air.

---

## **✶ TurboTax potential overstatement of gross income**

Richard Mason <mason@unr.edu>

*Thu, 01 Mar 2001 14:41:45 -0800*

In using TurboTax there is an ability to directly download income tax information on dividends, interest and securities sales, from various brokerage firms directly into TurboTax. When downloading income tax information from Fidelity Investments for a joint tax return I ended up with duplicate, i.e. double amounts of interest and dividends, in the following circumstance. Husband and wife each have individual brokerage accounts. They also have a joint brokerage account. Husband's account info downloads into TurboTax on his social security number and password, wife's account information downloads into TurboTax on her social security number and password. Joint account information downloads on each access. The result is a doubling of the interest and dividend income into TurboTax. This may be unique to the Fidelity account access system that allows joint account access from either social security number and password, but it is a concern.

Richard Mason, University of Nevada

---

## **⚡ Risks of buggy cell phone networks**

<kragen@pobox.com>

*Fri, 2 Mar 2001 02:22:56 -0500 (EST)*

I've been a customer of Sprint PCS in Silicon Valley since mid-January.

I've noticed that, frequently, when I call busy phone numbers, I never hear

a busy signal; instead, I hear my own voice echoed back at me.

My morning train seatmate had a Motorola Sprint PCS phone she claims works

everywhere but San Francisco. Here, whenever she called her Sprint PCS

voice mail (located in Texas), she got connected to someone else's

in-progress call --- apparently selected at random.

I observed the same phenomenon later today trying to call my girlfriend's

Seattle Sprint PCS phone and (non-Sprint, non-cellular) home phone.

Sometimes I got fast busy signals, sometimes I got my own echo, and

sometimes I got other people's conversations. It appeared that I was only

hearing one side of the conversation, the speakers could not hear me, and my

listening did not disrupt their conversation; but it only lasted for ten

seconds or so. Still, I heard snatches like, "Yeah. She says this is the

sickest she's ever felt." One eavesdropping session lasted nearly a minute.

I suspect these are two manifestations of a single bug in Sprint's base station software. I wonder who's listening in on my conversations? This (plus Sprint billing me \$161 for my first day of service, then \$99 for the next 30 days) will probably wean me from Sprint.

Any secure communications architecture that relies on hop-by-hop encryption will be vulnerable to bugs like this in switches. End-to-end encryption is more robust against such things.

---

## SETI@Home felled by a Single Point of Failure

Malcolm Pack <risks2@potnoodle.net>

*Thu, 01 Mar 2001 07:35:22 +0000*

After being unavailable for over 24 hours, the home page for the SETI@Home project, <<http://setiathome.ssl.berkeley.edu/>>, has currently (1 March 2001) been set to redirect to a holding page at <<http://www.net.berkeley.edu/setiathome/>>.

| Fiber cut silences SETI@Home

| At about 3:30 AM PST on 27 February an optical fiber cable connecting

| the U.C. Berkeley campus with the Lawrence Berkeley National Laboratory was cut, apparently by vandals trying to "salvage" copper

| from other nearby cables.

| The broken fiber carries data and voice connections for LBNL and also

| for the Space Sciences Lab. SSL is where the SETI@Home project

is  
| located, so the millions of participants helping to analyze  
data have  
| been unable to contact the SETI@Home servers for more than a  
day.  
|  
| Contractors are pulling new cable now. It's expected that  
service to  
| SSL will be restored by Friday, 2 March 2001. We'll update  
this page  
| as we learn more about the progress of the repairs.

I infer either:

o Traffic to and from the SET@Home servers is too great to  
be  
permitted to use any backup connection that exists  
between the  
two facilities.

or

o LBNL and SSL are cut off from the 'Net altogether until  
this  
SPF is repaired.

The loss of processing time to the project is unimportant in  
terms of  
contribution to overall success or failure (I doubt ET will be  
too  
upset if we find him/her/it/them 4 days later than expected),  
but the  
drop-out rate may increase as people simply give up instead of  
checking the home page for an explanation for their lack of  
progress.

Malcolm Pack

---

**✶ Passwords don't protect Palm data, security firm warns**

Yves Bellefeuille <yan@storm.ca>

Fri, 02 Mar 2001 17:41:00 -0500

At <http://news.cnet.com/news/0-1006-202-5005917-0.html>:

Passwords don't protect Palm data, security firm warns

By Robert Lemos

Special to CNET News.com

March 2, 2001, 11:45 a.m. PT

<http://news.cnet.com/news/0-1006-201-5005917-0.html?tag=prntfr>

People who rely on passwords to keep strangers from poking through the data stored on their Palms actually have no protection at all, a network security company warns.

In an alert posted Thursday, @Stake pointed to a back door in the Palm operating system that allows anyone with developer tools to access data on handhelds that have been "locked" with a password.

If someone finds or steals a Palm, the owner's data is basically an open book. And the theft of mobile devices for their data is becoming more common.

"This is the nail in the coffin of the notion that the Palm has any security for your data," said Chris Wysopal, director of research and development for Cambridge, Mass.-based @Stake.

"Any attacker with a laptop and a serial (syncing) cable is pretty much able to access everything on the device," he said.

Handspring's Visor handhelds and Sony's Clie use the Palm OS.

Palm representatives would not immediately comment on the advisory.

The security flaw is actually in the OS for a reason. Palm software engineers and many of its application developers use the back door to debug applications running on the handheld. Many of them do not consider it to be a security issue, Wysopal said.

However, few people who use the devices realize that using a password will keep only the casually curious from looking at their data.

For that reason, @Stake said, it released the warning.

"It's equivalent to adding a password to your PC's screensaver. "There's no true security in that," said Wysopal, who is known in the security community by his hacker handle, Weld Pond.

Last September, @Stake discovered that the encrypted password used by Palm OS to protect so-called private records from prying eyes could easily be broken. With the discovery of the latest back door, it would seem that no data is safe.

With a laptop loaded with developer tools and a sync cable, anyone who obtains access to a handheld can access the owner's data, add or delete applications, and format the memory card.

Even Palm handhelds protected by encryption software could be compromised by using the back door to load a program to record all passwords as they are entered.

Wysopal warned that weak Palm security could lead to other

compromises  
as well.

"You have corporate administrators keeping their company's critical passwords on their Palm because they think it is secure," he said.

The back door affects all current versions of the Palm OS, Wysopal said. Palm OS 4.0, due later this year, is expected to correct the problem.

Yves Bellefeuille <yan@storm.ca>, Ottawa, Canada

---

## ⚡ Risks of laptop anti-theft devices

Tony Yip <tonyy@chancery.com>  
*Mon, 5 Mar 2001 12:01:30 -0800*

Edited slightly from Burnaby Now, March 4, 2001, page 8.

Nearly 300 people were evacuated from "the boot" (the phone company's main office building) last Monday after an employee mistook a computer's anti-theft device for a bomb.

Spokesman said police were called to the company offices around 4:45 pm to investigate a small beeping object wrapped in tape that was left in the men's washroom.

Investigators examined the device and determined the little bundle was nothing more than a loss prevention device removed from one of the company's laptop computers.

Police have since learned that when the device was removed, frustrated employees tried to muffle its persistent alarm noise by wrapping it in tape. When that effort proved fruitless, one of the workers stashed the alarm in the washroom "for a little peace and quiet." "The guy walking in there afterwards must have had some scare. Thankfully this wasn't the real thing, but you should always be aware of your surroundings... you can never be too careful."

---

## ✶ Where does NAVSTAR say we are, again?

James Paul <James.Paul@mail.house.gov>

*Fri, 2 Mar 2001 13:52:07 -0500*

OS/COMET, top-secret U.S. computer-system source code for guiding spacecraft, rockets, and satellites, has been obtained through an Internet

breakin at the U.S. Naval Research Laboratory in Washington D. C., traced to

a company in Stockholm and then to someone with username LEEIF (seemingly in

Germany) masquerading as a user of freebox.com. This software is used in

NAVSTAR GPS monitoring. [Source: Hacker gets hold of top secret U.S. space

codes, Reuters News Service, 2 Mar 2001; PGN-ed; see also

<http://www.washingtonpost.com/wp-dyn/articles/A16751-2001Mar2.html>

<http://www.washingtonpost.com/wp-dyn/articles/A16751-2001Mar2.html> ]

## **⚡ Beware assumptions about keyboard layouts...**

"Perry Pederson" <perandtim@home.com>

*Fri, 2 Mar 2001 08:30:00 -0800*

I recently started a checking account at Hewlett-Packard's credit union, and as part of the process of obtaining a VISA debit card attached to the account, I needed to create a four digit PIN number for the card. After the card was initialized at the credit union, it failed to work at ATM machines, giving me an "invalid PIN number" error. I re-initialized the card three different times with credit union personnel, to no avail. Finally, after several calls to the credit union's main office to determine why my PIN wasn't taking, I noticed that the keypad that I used at the credit union to set the PIN number had the rows appearing in the opposite order of a "normal" PC keyboard-- the topmost row of keys had the numbers "123", the second row "456", and the third row "789". When I was generating my PIN, I was automatically pressing keys that had the same pattern as an "old" PIN that had I used at a previous bank without checking the numeric values associated with the keys. Once I entered the "correct" numbers, the card worked fine at ATM machines.

The RISKS here should be obvious-- one should observe the input hardware being used, regardless of how similar it may look to other input devices.

**Re: On paper-size standards (Klossner, [RISKS-21.25](#))**

Gideon Sheps <gbs@asiabondportal.com>

Wed, 28 Feb 2001 10:40:31 +0800

> Other disparaging remarks, such as the "bizarre" way that we  
> norteamericanos measure paper density, would perhaps be more  
compelling if  
> they did not come from an island where everyone drives on the  
wrong side  
> of the road.

I would be more inclined to be sympathetic if America wasn't the  
only  
country in the world still using the "British Imperial Standard  
of Measure"  
based on such sensible units such as the length of the King's  
foot or  
distance from his thumb to nose with arm outstretched, some 225  
years after  
their revolution.

Further, the whole world hardly drives on the same side of the  
road as the  
USA - in fact, as you might discover, the Brits are hardly  
alone. The  
Japanese, as well as much of Asia, Australia, New Zealand, parts  
of Africa,  
(e.g., S. Africa), and the Carribean (Bermuda, Bahamas, BVI...),  
also drive  
on the right.

Given that India and Indonesia drive on the right, which roughly  
match China  
for population, I'd say its a tight race for the question of who  
is really  
on the wrong side.

Technically, the Brits are on the correct side of the road, as approaching your opponent with your right hand free to hold the lance or sword is preferential for the 85% of the population who are right handed. (make that Gun for Americans... one might ask how many fewer random drive-by shooting victims might there be if they were firing with the right instead of left hand and could aim better?).

I think the real risk here is that American schools don't prepare Americans for life outside America.

G. Sheps (A "nortamericano" in Hong Kong)

---

## **REVIEW: "Tangled Web", Richard Power**

"Rob Slade, doting grandpa of Ryan and Trevor" <rslade@sprint.ca>  
*Mon, 26 Feb 2001 08:25:15 -0800*

BKTANGWB.RVW 20001027

"Tangled Web", Richard Power, 2000, 0-7897-2443-X,  
US\$25.00/C\$37.95/UK#18.50

%A Richard Power  
%C 201 W. 103rd Street, Indianapolis, IN 46290  
%D 2000  
%G 0-7897-2443-X  
%I Macmillan Computer Publishing (MCP)  
%O US\$25.00/C\$37.95/UK#18.50 800-858-7674 317-581-3743 www.mcp.com  
%P 431 p.  
%T "Tangled Web: Tales of Digital Crime from the Shadows of Cyberspace"

This book gives a reasonably balanced review of the perception

of security experts in regard to the level of computer or communications involved crime going on in our networked world. That is because this is not so much a book, as an extended compilation article. Power reproduces interviews with, or grabs quotations from the written works of, a great many forensic and security specialists or researchers. Very large chunks of the book are taken from previously published works.

Note also that I say "balanced," and not "complete."

Part one appears to be intended as a general introduction to computer related crime. Chapter one is the usual statement that it goes on, mercifully brief. Despite an interview with Sarah Gordon and extensive quoting from Donn Parker, chapter two's look at cybercriminals focuses rather narrowly on the fact that people who do crimes aren't normal. The CSI (Computer Security Institute)/FBI Computer Crime and Security Survey is introduced with many graphs and tables in chapter three. The description does mention, but doesn't emphasize, the fact that the survey was self-selecting and self-reporting, and therefore only marginally more informative than an opinion poll. Chapter four tries to look at costs.

The title of part two seems to indicate a deeper analysis of criminals and system breakers. Chapter five touches on the infamous Operation Sundevil (the law enforcement disaster that was the inspiration behind Bruce Sterling's "The Hacker Crackdown," cf. BKHKRCRK.RVW), and the even more

infamous Morris Internet Worm: is Power trying to equate police activity with system breaking? Three penetration episodes that led to the arrest of young crackers are described in chapter six. Some stories of theft of credit card numbers, bank fraud, and advanced phone phreaking are given in chapter seven, but these are cobbled together from published interviews with police, and have little technical background. There is a little bit about nuisances and vandalism, and a lot about distributed denial of service, in chapter eight. Chapter nine tells the stories of the Melissa and Love Bug e-mail worms. As with the earlier tales in the book, the material is technically weak, and has other errors of fact as well. (I exclude the respective CERT advisories, which are reproduced in full.)

Part three is about spies and espionage. However, chapter ten, which talks about spies, doesn't really have anything to say about computer penetration. The stories are all very terse mentions of spying culled from general news reports. The tales of insider fraud, in chapter eleven, vary in length and don't really present any more than trivial information. Infowar gets a mix of anecdotes and speculation in chapter twelve.

Part four looks at personal attacks. Both chapter thirteen, on identity theft, and chapter fourteen, on child pornography, are short and oddly unhelpful.

Part five turns to defensive activities. Chapter fifteen concentrates on where the security department should be on the corporate org

chart. Global law enforcement recounts a few presentations by non-US law enforcement people in chapter sixteen. There are more details on US government security offices and activities, in chapter seventeen, but not many. Countermeasures, in chapter eighteen, is a "once over lightly" of the entire security field. The epilogue, entitled "The Human Factor," is vague.

If you haven't been paying any attention to computer security, this book is a quick read that will get you a very rough idea of what is going on in the areas of greatest concern to large corporations. If it scares a few people that will be all to the good: it certainly doesn't help you to start doing anything about security. Presumably it is the general public, with little knowledge of computer security, that is the intended audience. However, the lack of structure and uneven quality and depth of information make it difficult to know what those readers will take from this book.

If, of course, you have been paying any attention at all, this is pretty old news.

copyright Robert M. Slade, 2001    BKTANGWB.RVW    20001027  
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 21: Issue 27**

**Thursday 15 March 2001**

## Contents

- [Stockholm power outage hits high-tech companies](#)  
[Ulf Lindqvist](#)
- [New USB Army 'Land Warrior' tech connects the next cybertoy](#)  
[Bob Frankston](#)
- [In Japan, do trains check for drivers?](#)  
[Joyce K Scrivner](#)
- [UCITA implements DoS and DDoS Vulnerabilities](#)  
[Warren Pearce](#)
- [Moon-landing-hoax hoax](#)  
[Dave Stringer-Calvert](#)
- [Mistaking list for scalar context brings cops](#)  
[Jamie McCarthy](#)
- [Fairfax, VA Police records public](#)  
[Dan Graifer](#)
- [Risks of would-be copper thieves](#)  
[Gregory Soo](#)
- [Yahoo! Mail translates attachments](#)  
[Bob Frankston](#)
- [More on Bibliofind](#)  
[Lenny Foner](#)

- [Re: Air Gaps](#)  
[M.S. Jaffe](#)
  - [Re: Smart bombs miss again](#)  
[Dave Aronson](#)  
[Randy Davis](#)
  - [Re: NAVSTAR](#)  
[PGN](#)
  - [Re: SETI@Home felled by a single point of failure](#)  
[George C. Kaplan](#)  
[Mary Schafrik](#)
  - [Re: When will they EVER learn?](#)  
[Gideon Sheps](#)
  - [Re: Palm passwords aren't...](#)  
[Peter Houppermans](#)
  - [Don't risk missing the Parnas Symposium at ICSE 2001!](#)  
[David Weiss](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

## ✶ Stockholm power outage hits high-tech companies

Ulf Lindqvist <ulf@sdl.sri.com>  
*Mon, 12 Mar 2001 10:58:49 -0800 (PST)*

As reported in various Swedish media, including \*Dagens Nyheter\* (<http://www.dn.se/>), Mar 12, 2001:

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 incident happened on Sunday morning, and utility company officials hoped that customers would have power again late Monday evening.

The largest employer in the area, Ericsson, told 11,000 employees to stay at home Monday as their workplace had no power. IBM did the same

thing for  
their 2,000 employees.

The blackout also caused problems with other depending services, such as water, heating, landline phones, mobile phones, pagers, Internet traffic and servers, and public transportation. Police and fire departments have been busy with burglaries (no lights or alarms working), fires (caused by candles and even indoor BBQs) and black traffic lights.

A spokesperson for the utility company Birka Energi says: "The cable damage is total. We cannot handle it with normal rerouting, because all the cables were destroyed."

All the cables in one tunnel, that is. Did anyone mention eggs and baskets?

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/>

[Egg-sell-ent time. That's what's called tunnel vision. PGN]

---

## ⚡ New USB Army 'Land Warrior' tech connects the next cybertoy

"Bob Frankston" <rmf2gOther@bobf.Frankston.com>

*Thu, 8 Mar 2001 13:50:14 -0500*

Apparently TransDimensions is a defense contractor that is using a version of USB (Universal Serial Bus) (and Bluetooth) as the basis for the

"Soldier-of-the-future" project. I can understand that some of the promised peripherals are "cool" and even useful. But one of the major lessons of the Internet is the power of the "end-to-end" approach that puts the onus on the end points to provide reliability. Bus architectures like USB provide a reliable and synchronous transport that is the basis for brittle designs that have little resilience. Unlike the Internet where each participant takes responsibility for quenching failures, in USB creates dependencies in which failures propagate. Of course USB also has the problem of not having an addressing structure for peer connectivity beyond a very local scale.

The problem is that stories about the soldier of the future are very glitzy and that it is easy to claim one needs a reliable networking technology such as USB rather than an imperfect one like IP. But that's like saying that you can't risk exposing children to germs because they might get sick. It works fine until the children are deployed (become adults). At that point they have no survivability.

<http://www.zdnet.com/anchordesk/stories/story/0,10738,2693677,00.html>

---

## **🚧 In Japan, do trains check for drivers?**

"Scrivner, Joyce K" <joyce.scrivner@unisys.com>

*Wed, 14 Mar 2001 19:24:28 -0600*

I thought checking for a driver on computerized trains was routine. They must not have deadman switches on Japan's bullet trains (Shinkansen). A driver left his seat to search for his misplaced hat -- because the company rules state that he must have his hat on at all times. Fortunately, (1) the train was going in the neighborhood of 15 miles per hour at the time, and (2) there were no passengers at the time. Drivers have now been informed that if they misplace their hat, they should continue to the next station.  
[Source: Bullet Train Left Driverless in Hat Search, Reuters, 14 Mar 2001]

---

## ✶ UCITA implements DoS and DDoS Vulnerabilities

"Pearce, Warren, CTR" <Warren.Pearce-contractor@jntf.osd.mil>

*Thu, 8 Mar 2001 07:48:08 -0700*

Ed Foster's "The Gripe Line" Column in the 5 Mar 2001 issue of \*Infoworld\* (www.infoworld.com) raises a pair of interesting Denial of Service (DoS) and Distributed Denial of Service (DDoS) attack vulnerabilities. He says:

Foremost among the perils posed by UCITA is the "electronic self help"

section that allows software publishers to equip their programs with

remote disabling capabilities.

Think about this in terms of a DoS vulnerability. The vendor may say that the capability is disabled for software bought with a Commercial

bulk

license. For example, Microsoft has indicated that they disable this "feature" for their bulk license sales. However, how can a DoD/Commercial user with a very critical application be sure that the process that disabled the remote disabling capability can't be circumvented? Consider the motivation an adversary would have for software used in critical DoD applications.

In another section of his Column, Ed commented (*\*Italics\* added by Warren Pearce*):

A perfect example is the service agreement posted by Juno in January, particularly the section in which Juno claims the right to use its customers' computers during their downtime to run its own "Computational Software". Juno's service agreement states, "In connection with downloading and running the Computational Software, Juno may require you to leave your computer turned on at all times. ... *\*You expressly permit and authorize Juno to initiate a telephone connection from your computer to Juno's central computers, ... and you agree that, as between you and Juno, you shall be responsible for any costs and expenses resulting from the foregoing.\** ... As has been widely reported, in February Juno announced its Virtual Supercomputer Project, which will harness its customers' unused CPU cycles to sell as a *\*distributed computing service.\**

Think about *\*distributed computing service\** as *\*distributed DDoS*

service\*.

Consider \**"You expressly permit and authorize Juno to initiate a telephone connection from your computer to Juno's central computers"*\* and you have only one telephone line to your house. This indicates that Juno can occupy this line at their volition? Hope you don't need to make a 911 call!!! The user \*shall be responsible for any costs and expenses.\* The lawyers and Juno will have fun after the DDoS attack.

W. Warren Pearce, CISSP, TRW System Security Engineer, Joint National Test Facility, Schriever AFB, CO. 80912 1-719-567-8736

---

## **✶ Moon-landing-hoax hoax**

Dave Stringer-Calvert <dave\_sc@csl.sri.com>  
*Wed, 07 Mar 2001 17:28:02 -0800*

Someone hacked a NASA Web site and replaced it with a conspiracy theory about the moon landings being faked.

<http://www.zdnet.co.uk/news/2001/9/ns-21426.html>

---

## **✶ Mistaking list for scalar context brings cops**

Jamie McCarthy <jamie@mccarthy.vg>  
*Wed, 14 Mar 2001 09:46:41 -0500*

A high-school sophomore last week was called to his private

school's office

and asked to explain some suspicious text on his Web site. What was

intended to be a quote from /usr/games/fortune was instead the \*first line\*

from its output. The school staff was very alarmed because the full output

would have been:

I put the shotgun in an Adidas bag and padded it out with four pairs of tennis socks, not my style at all, but that was what I

was aiming for: If they think you're crude, go technical; if they

think you're technical, go crude. I'm a very technical boy. So I

decided to get as crude as possible. These days, though, you have

to be pretty technical before you can even aspire to crudeness.

- Johnny Mnemonic, by William Gibson

Using a variable in list context on the left side of a perl expression

puts the right side into the same context, and many operators behave

differently in different contexts. These two statements are not equivalent:

```
my $f = `fortune`; # returns fortune as scalar, stores in $f
my($f) = `fortune`; # returns each line of fortune as one
element
                    # in a list, stores first line in $f
```

Only the line about the shotgun in the Adidas bag made it to this kid's Web

page, and the school went into crisis mode. They called the police just to be on the safe side.

<http://slashdot.org/article.pl?sid=01/03/13/208259>

Everything was eventually explained to their satisfaction, but

the cops  
still talked to this sophomore and his father for a couple of  
hours and  
they're keeping his name on file... again, "just in case."

The risk is, I think, being a private high-school student a week  
after a  
high-profile school shooting, and having a Web site.

Jamie McCarthy jamie@mccarthy.vg <http://jamie.mccarthy.vg/>

---

## **✶ Fairfax, VA Police records public**

Dan Graifer <dan@ad-co.com>  
*Mon, 12 Mar 2001 13:26:46 -0500*

The "Dr. Gridlock" column in the March 12, 2001 Washington Post  
(a regular  
column devoted to traffic issues in the DC Metro area)

[http://washingtonpost.com/wp-dyn/articles/A55582-  
2001Mar11.html](http://washingtonpost.com/wp-dyn/articles/A55582-2001Mar11.html)

points out that that Fairfax County police are posting their  
arrest records  
online. Everything from speeding tickets to homicide. It also  
notes that  
these are never updated to indicate the disposition of the  
cases, nor is  
that information available elsewhere.

Besides the URL provided:

<http://www.co.fairfax.va.us/ps/police/reports/Arrest.txt>

going up one level yielded a directory of what appears to be all  
the crime  
reports as MSWord documents. Note that this information has  
always been

publicly available, but you used to have to go to the police station to browse it.

The risks of this have been discussed before. I'd sure hate to be mistakenly arrested. "no really, that case was dismissed...". Sure hope that server is secure too...

Daniel A. Graifer <Dan@AD-CO.com> Home/Office: (703)425-6091  
Andrew Davidson & Company, 520 Broadway 8th FL, NY 10012 (212)  
274-9075

---

## **✶ Risks of would-be copper thieves (Re: SETI, [RISKS-21.26](#))**

"Gregory Soo hotmail" <grsoo@hotmail.com>  
*Sat, 10 Mar 2001 20:52:55 -0500*

Another copper-theft attempt shut down the Rogers@Home cable Internet service in Canada on 8Mar2001 for over 12 hours, although the thieves wound up only with fiber-optic cable carrying Internet traffic to a U. S. backbone. Over 300,000 Ontario subscribers were affected, because of an outdated backup system and a single-point vulnerability. [Source: Vito Pilienci, \*The Ottawa Citizen\*, 10Mar2001, Rogers@Home: First cut is the deepest. Rogers admits 'rather outdated' network vulnerable to bumbling thieves; PGN-ed  
<http://www.ottawacitizen.com/hightech/010310/5075158.html>]

[Coppers, robbers, backups, backbones, backhoes, back to basics. PGN]

## ✶ Yahoo! Mail translates attachments

"Bob Frankston" <rmf2gOther@bobf.Frankston.com>

*Tue, 6 Mar 2001 20:50:38 -0500*

I thought the RISKS readers would find this ZDNet item excerpt entertaining:

BugNet, with testing help from KeyLabs, has validated a quirk in the

Yahoo! Mail online attachment viewer that translates certain words when

they are displayed in a browser. Even though these word conversions will

hardly be noticed by most Yahoo! Mail users, it has caused some confusion

with others, and it is probably good that you be aware of what is going on.

<http://www.zdnet.com/zdhelp/stories/main/0,5594,2631218,00.html>

[Unfortunately, the two-paragraph item contains no examples. PGN]

---

## ✶ More on Bibliofind ([RISKS-21.26](#))

Lenny Foner <foner@media.mit.edu>

*Mon, 5 Mar 2001 18:02:42 -0500 (EST)*

Mere moments after sending my previous message, this landed in my mailbox.

It still doesn't answer the question of why they were retaining any of this

information in the first place; I've asked them why, but don't expect a

response, since they'll presumably be deluged.

(Given that there seemed to have been no way, for example, to add or subtract a credit card [because there was no way to discover that Bibliofind knew about me as a particular user -at all-; it remembered my state on a couple of forms as I filled them out, but presumably forgot all about me as soon as the final form was submitted], and since not all booksellers accept all cards, one might have thought that Bibliofind wasn't keeping any of this information. This seems a great example of a site just hoovering up info for some ill-defined later purpose that they didn't need at all. When, oh when, will such sites learn that this behavior only serves as (a) a cracker target or (b) a way to waste money answering subpoenas?)

- - - Begin forwarded message - - -

Date: Mon, 05 Mar 2001 12:03:02 -0500  
From: info@bibliofind.com  
To: info2@bibliofind.com  
Subject: Important Information from Bibliofind

Dear Bibliofind Customer:

Bibliofind has just learned of a security violation on its site that compromised the security of credit-card information used on Bibliofind's servers from last October through February 2001.

We have no information at this time to suggest that your credit card has been misused, but we wanted to notify you as a precautionary measure. We have been in contact with the federal law enforcement authorities on this

matter, and we have also notified the appropriate credit card companies, so that they can take the necessary steps to protect the interests of any cardholders who may be affected.

If you have specific questions about your credit-card account, please contact the issuer of your credit card.

To ensure this doesn't happen again, we have removed all customer credit-card information, physical addresses, and phone numbers from Bibliofind's servers. We expect to bring the Bibliofind system back into operation shortly.

We apologize for any inconvenience this may cause you. You can contact us with questions at [info@bibliofind.com](mailto:info@bibliofind.com).

Sincerely,

Bibliofind

---

## ✉ **Re: Air Gaps (Schneier, [RISKS 21.26](#))**

"M.S. Jaffe" <[jaffem@pr.erau.edu](mailto:jaffem@pr.erau.edu)>  
*Tue, 13 Mar 2001 21:34:50 -0700*

> ... Nonetheless, the intruder can still access the back-end server as a  
> regular client. The intruder can still break into the internal system by  
> exploiting any vulnerabilities above the transport layer. ...

Mr. Schneier is, of course, quite correct. And, as far as I am concerned,

his observation, above, should be printed on almost every computer security product marketed today --- something like the Surgeon General's warning on tobacco products. It is also worth remembering that even \*real\* air gaps cannot totally prevent the leakage of sensitive information (or, in theory, going the other direction, possible attacks). An air gap might reduce covert channel bandwidth dramatically, but it cannot reduce that bandwidth to zero.

... Matt

<http://backoff.pr.erau.edu/jaffem>

---

## **⚡ Re: Smart bombs miss again (Lord Wodehouse, [RISKS-21.26](#))**

Dave Aronson at bigfoot dot com or att dot net <postmaster@airnsun.dcfido.org>  
*Tue, 13 Mar 2001 08:50:45 -0500*

> The military rely on ["smart weapons"] more and more, and  
> yet they are shown to be more limited and often less usable.  
> Extending this on to the smart guns and systems for soldiers,  
> I see the fighting forces becoming less effective.

And not only soldiers. Though the "smarts" are of a different variety (user authentication versus targeting), the probable faults of so-called "smart guns" are a hot topic within the gun control debate. Even setting aside the question of civilians, would you want police (who are more often shot with their own guns than any other, in the USA), never mind the military, armed with such technology? Some designs deactivate the gun if the battery dies;

soldiers may maintain their weapons well (even in peacetime, for fear of discipline), but police (at least here in the USA) are infamous for not doing so. Many designs are even susceptible to jamming signals easily generated with a handheld device (which of course will be a hot item, so to speak, among criminals). Some require punching in a code in order to activate the gun... and of course the keypads (another point of failure) have to be small (to fit) and difficult to depress (to avoid false presses during normal handling), so the chances of fumbling under the stress of having your life in immediate danger are greatly magnified. The list of risks goes on....

---

## ✶ **Re: Smart bombs miss again (Lord Wodehouse, [RISKS-21.26](#))**

<Randy Davis>

*Tue, 6 Mar 2001 00:31:54 -0500*

> "Pentagon officials have admitted that most of the bombs  
dropped by US  
> and British warplanes on Iraq last Friday missed their  
targets."  
> [...]  
> Yet again I find myself writing to RISKS to point out that  
these  
> computer-game type weapons are almost always oversold on their  
abilities

Independent of whether the weapons are being oversold, I find myself writing to RISKS yet again to point out the meaninglessness of the

statistics cited.

Consider first of all the word "most," used presumably because it sounds impressive. If you read the BBC article you discover that what they mean: "bombs hit fewer than 50% of the targeted radars." So if 49% of the bombs hit, "most" of them missed.

Now consider "fewer than 50%" as a bomb hit rate. Is that great, ok, or terrible? Right, you don't know.

Third, it's a doubly meaningless statistic. One relevant point is, compared to what? The comment in 21.26 claimed in passing that they "have been little more effective than plain dumb bombs." Really? What's the accuracy of plain dumb bombs? Is it 49%? No doubt some folks in the audience actually know the answer to that and can supply it, but the BBC report didn't say and neither did the Risks posting.

The second half of the meaninglessness is that accuracy isn't measured as hit or miss; bombs (and missiles) don't have to hit the target to be effective. Sometimes 2000 pounds of explosive going off in even the general neighborhood is quite enough.

One standard measure is "circular error probable," a circle within which 50% of the bombs would fall. The relevant statistic is the size of that circle. One source indicates that in WWII, "more than half the bombs dropped missed their targets by well over 1000 yards" (<http://www-cgsc.army.mil/usaf/Pubs/Enemysystem.htm>), i.e., they fell more than half a mile from the target. How much better is

conventional bombing  
now, and how do the smart bombs compare? That would be an  
interesting set of  
numbers.

In the absence of the relevant numbers and relevant comparison  
points, the  
widely repeated "more than 50%" is simply meaningless, no matter  
how  
melodramatic it sounds.

Randall Davis

---

**✉ Re: NAVSTAR (Paul, [RISKS-21.26](#))**

Peter Neumann <neumann@csl.sri.com>

*Mon, 5 Mar 2001 20:28:50 -0500*

I have been informed that \*The Washington Post\* article says,  
"An FBI  
spokesman said that the stolen software was unclassified." PGN

---

**✉ Re: SETI@Home felled by a single point of failure (Pack, [RISKS-21.26](#))**

"George C. Kaplan" <gckaplan@ack.Berkeley.EDU>

*Mon, 12 Mar 2001 17:10:38 -0800*

If there had been a (lower speed) backup link we could have  
applied  
rate limits to the SETI@Home traffic, to keep it from swamping  
the  
link. Granted, this may have been almost indistinguishable from

blocking the SETI@Home data server altogether, but it would have allowed other SSL net traffic to get through.

> LBNL and SSL are cut off from the 'Net altogether until this  
SPF is  
> repaired.

This is only partly true. The severed cable connected LBNL to the UC Berkeley campus. LBNL has other connections to the Internet, so they were not completely cut off. SSL and the Lawrence Hall of Science are administratively and topologically part of UC Berkeley, even though LBNL lies between them and the rest of campus. They *\*were\** completely cut off from the net for about 5 days.

> ... drop-out rate may increase as people simply give up instead of  
> checking the home page for an explanation for their lack of progress.

I don't have any information on drop-outs, but the data volume has returned to normal levels since the cable was repaired, so I'd guess the impact was minimal. The disruption to the everyday business of SSL and LHS was undoubtedly much worse than the overall effect on the SETI@Home data processing.

There were some interesting side effects. SETI@Home has a LOT of users. Even though only a tiny fraction went to the trouble of looking up contact information for UC Berkeley, we were getting a steady stream of e-mail queries asking why SETI@Home was off the air. We redirected their Web server traffic to that status page in order to cut down on the number of

queries.

The redirection had the intended effect. However, we used one of our standard Web page templates for the status page. The template includes some links to our own Web pages, such as the one for job listings in our department. So that's why we saw a big increase (an order of magnitude) in the number of employment inquiries during the outage.

George C. Kaplan, Communication & Network Services, University of California  
at Berkeley 1-510-643-0496 gckaplan@ack.berkeley.edu

---

## **⚡ Re: SETI@Home felled by a single point of failure (Pack, [RISKS-21.26](#))**

Mary Schafrik <mschafrik@cintechsolutions.com>  
*Tue, 6 Mar 2001 13:30:41 -0500*

Even if they had a backup line, it's very likely that it was bundled in the same cable as the primary line. Even if you order service from several vendors, they usually use the same physical bundles into your building.

---

## **⚡ Re: When will they EVER learn? (Kuenning, [RISKS-21.25](#))**

Gideon Sheps <gbs@asiabondportal.com>  
*Tue, 06 Mar 2001 15:42:04 +0800*

We had the other side of this problem at our site.

We generate and e-mail an initial random string password to ensure that a user has at least supplied us with one piece of valid, somewhat traceable, information.

Since we have no choice but to send it back in e-mail we did NOT include the login name, which the user has chosen themselves, in that e-mail.

Thus, if the e-mail was seen (we figure there is more chance of it been seen on the office printer than by a sniffer) at least one essential element was still missing.

Well, what happened next was that customer service started getting e-mail and calls from users who could not recall what login name they had selected!

I should add that the password is generated and e-mailed immediately, and will normally arrive in someone's inbox no more than a minute after they complete the sign up.

We have also had to gradually reduce the efficacy of the random string, as customer service requested we eliminate numbers and mixed case because of the number of calls they fielded because of "shiftkeyanemia".

Our site only serves professional bond traders, investment managers, bankers and such. Not the general public.

## **⚡ Re: Palm passwords aren't... (Bellefeuille, [RISKS-21.26](#))**

Peter Houppermans <Peter.Houppermans@paconsulting.com>

*Tue, 6 Mar 2001 13:35:56 -0000*

Re: Passwords don't protect Palm data, security firm warns (Yves Bellefeuille)

Neither do they on a Psion Series 3 or 5 if you have left the serial link on. If the device is locked by password it is still possible to access the device in full if the serial link has been left online. And I don't think I'd need to point at the obvious risk of storing your data on removable media which are not subject to the password lock if plugged into another machine ;-).

However, there is hope here: you can always protect the individual files by running a crypto program over it - whilst accepting that PDA security could be improved. I use a Psion Series 5MX with an RSA based freeware program ("crypto" - <http://salvis.com>) which works and integrates well. Is it safe? I wouldn't think so, but it will protect the information that little bit longer from casual disclosure.

Peter Houppermans <peter.houppermans@paconsulting.com>

---

## **⚡ Don't risk missing the Parnas Symposium at ICSE 2001!**

David Weiss <weiss@avaya.com>

*Wed, 7 Mar 2001 17:47:28 -0500*

[Dave Parnas is one of our most distinguished participants with respect to his efforts to prevent risks. His positions on the Strategic Defense Initiative were noted in our very first issue [RISKS-1.01](#), and he made numerous contributions throughout the early RISKS volumes, including 1.02, 1.06, 1.08, 1.28, 1.35, 1.36, and 1.37. This birthday celebration falls in the midst of the IEEE Security and Privacy Symposium, but I hope many of you will be at ICSE 2001 and able to attend. PGN]

Dan Hoffman and I are organizing a Symposium at ICSE 2001 recognizing Dave Parnas's work and in honor of his 60th birthday. David L. Parnas Symposium, A special event at the International Conference on Software Engineering ICSE 2001 Tuesday 15 May 2001, Toronto, Canada <http://www.islandnet.com/~dlps>

This symposium is being held in recognition of Parnas's work and in honor of his 60th birthday. It is an opportunity for everyone in the software engineering community to celebrate his contributions and to think hard about where we are today and where we are going.

The symposium program includes

- \* keynotes by Fred Brooks and Jon Bentley
- \* invited talks by Jo Atlee, Paul Clements, and Jim Waldo
- \* a short presentation by Parnas
- \* a panel on software engineering education

Each symposium attendee will receive a copy of the book Software Fundamentals: Collected Papers by David L. Parnas, a new book from Addison-Wesley.

Dave Weiss



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 21: Issue 28

**Tuesday 20 March 2001**

## Contents

- [Aasta train crash might have been caused by a safety-critical error](#)  
[Anton Setzer](#)
- [Lax security found in IRS electronic filing system](#)  
[Dave Stringer-Calvert](#)
- [Dow Jones Industrial Average reported at 0.20](#)  
[Lindsay F. Marshall](#)
- [More on the importance of safeguarding private crypto keys](#)  
[David Kennedy](#)
- [Risks of self-induced false alarms](#)  
[Graystreak](#)
- [Using automation software without accounting for possible scenarios](#)  
[Tony Yip](#)
- [Another "secure" e-book seems unlikely](#)  
[Moz](#)
- [The risks of accidentally becoming a customer for life](#)  
[Jim Youll](#)
- [NSF study: "Internet Voting is no 'Magic Ballot'"](#)  
[Terry Carroll](#)
- [On-line elections](#)  
[Sarr Blumson](#)

- [Smart Bombs - Old Story](#)  
[Bruce E. Wampler](#)
  - [Re: Smart bombs miss again](#)  
[Richard Schroepel](#)  
[Christophe Augier](#)  
[Pekka Pihlajasaari](#)  
[Michael Nelson](#)  
[Bill Stewart](#)  
[Wm. Randolph Franklin](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

## ✶ Aasta train crash might have been caused by a safety-critical error

anton setzer <a.g.setzer@swansea.ac.uk>

*Sun, 12 Nov 2000 01:09:06 GMT*

[Archive note: overstruck ringed "A" in "Asta" lost in transit. PGN]

An extremely detailed report on the Aasta train crash in Norway, 4 Jan 2000, in which 19 people died is now available via <http://odin.dep.no/jd/norsk/publ/rapporter/aasta/>

Most of it is in Norwegian, but a Summary (pages 275 ff in "12. Sammandrag" at "Del 4") and in the appendices ("Vedlegg") Vedlegg 4 and Vedlegg 5 are very detailed reports on the Signalling installations there in English.

To remind you of the accident (which is described in the summary in detail):

the accident happened on a single-track line. Two passenger trains, a fast train and a small local train were about to meet. Both left at stations where trains can bypass each other. The fast train had a green

signal. The local train was supposed to have a red signal. The trains crashed in between. What was tragic was that both trains were on collision for 4 minutes which was indicated by the train controlling system, but the controllers didn't realize it in time and then didn't have the correct mobile telephone numbers of the trains.

Some points I found interesting are:

On page 277 of the main report one can read:

"In the light of the above, the commission cannot state with certainty what signals were showing on the northbound line at Rudstad station on 4 January 2000. From a technical point of view, it would seem highly likely that a red exit signal was showing. At the same time, the design of the safety system makes the potential for error so great that the commission cannot with certainty exclude malfunction situations that may have produced a different signal aspect."

In the report by SINTEF (appendix 4, English version page 53 ff) a long list of known deficiencies is listed.

4 incidents are listed: one in which a signal showed green, although it should have shown red (page 56 ff in the report by SINTEF), one occurring on 18 Apr 2000, after the train accident. 3 of them seem to indicate that under certain circumstances for a short time erroneously a green light is shown. (One incident seem to have been caused by mechanical problems).

SINTEF apparently did a by hand analysis of the accident and couldn't find an error.

In attachment 5, the report is assessed by Railcert, and SINTEF's report is criticized (section 6.1):

"We feel that Sintef's conclusions 2, 4 and 6 suggest that a technical cause, related to the signaling installation, for the accident can be ruled out. We support this conclusion only inasmuch as it applies to a steady state, single cause failure. We do however stress the need to look beyond such "simple causes".

"In fact Sintef's studies have revealed a number of deficiencies in the design of NSB87 (and NSI-63) as well as serious hiatus in the collection and safeguarding of possibly vital evidence immediately after the accident. A number of known reports of anomalies in similar installations exist. Based on these, we have been able to construct theoretical scenarios where the behaviour of the signaling installations might at least have contributed to the causes of the accident. These scenarios as well as effects of combinations of several known deficiencies could neither be proven, nor disproved by the evidence in hand, or the result of Sintef's analyses and studies.

\*\*\*\*\*

When looking at the data I found the following interesting:

- 3 of the incidents seem to have to do with the fact that the signal system

sometimes shows green light for short amount of time although it should

show a red signal (one further incident has to do with hanging green light).

- It is very strange that the local train which according to the log must have driven over a red light left 3 minutes earlier.

- It might be that a train drives over a red light while running. In the situation in question however, the local train was waiting at a station, and when waiting in front of a red light, it is unlikely to drive over it.

- The fast train and the local train left at almost the same time: The fast train passes the main exit signal at Rena at 13:06:15. The local train leaves Rudstad platform at 13:06:17 and passes the main exit signal at Rudstad at 13:06:58.

From this I conclude that the following scenario might have happened:

- When switching to green, under certain circumstances, the signalling system erroneously issues for a short moment a green signal to the opposite signal of the block as well.

- The driver of the local train interprets this as an indication that he should drive now in order to bypass the other train in time at the other station. Rudstad. The driver doesn't check the signal again, which probably, when passing the exit signal, already has switched back to red.

- If this was the case, this accident is due to a software error.

Of course the above is highly speculative and I haven't read the report in detail (especially the Norwegian part). I can imagine as well that the driver of the local train behaved abnormally caused by sleepiness, mental problems, irritation by sun light.

I think it would be very interesting to try to find the cause of this accident, in which a software error led to the loss of 19 lives.

Anton Setzer, Computer Science, University of Wales Swansea,  
Swansea SA2 8PP

UK <http://www-compsci.swan.ac.uk/~csetzer/> +44 1792 205678 ext  
4518



Dave Stringer-Calvert <dave\_sc@csl.sri.com>

*Fri, 16 Mar 2001 07:27:00 -0800*

Even as the IRS was assuring taxpayers last year that electronic filing of tax returns was secure, serious shortcomings existed that could have allowed hackers to view and even change information on returns, a government watchdog agency said. The General Accounting Office found no evidence that hacking had occurred, but it said its investigators were able to gain unauthorized access to the tax agency's electronic filing system, which will handle a third of all federal returns this year. The GAO cited the IRS for lax security controls and for not requiring encryption of

electronic returns. The report also said the IRS sent out \$2.1 billion in refunds to taxpayers whose returns were not properly authorized.

<http://www.latimes.com/business/20010315/t000022659.html>

[http://www.msnbc.com/news/TECH\\_Front.asp](http://www.msnbc.com/news/TECH_Front.asp)

<http://www.usatoday.com/life/cyber/tech/2001-03-15-e-filing-risks.htm>

<http://www.cnn.com/2001/US/03/08/taxes.electronic.filing/>

---

## 🚀 Dow Jones Industrial Average reported at 0.20

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

Mon, 19 Mar 2001 19:46:37 +0000 (GMT)

Oops! Lindsay <http://catless.ncl.ac.uk/Lindsay>

(From DATEK online:)

Monday, 19 March 2001, 4:53:47am

```
-----  
DJIA           0.20           -10031.08  
NASDAQ        1890.91           -49.80  
S&P 500       1150.53           -23.03
```

[Source: Article by Kieren McCarthy, 19 Mar 2001, \*The Register\*:

<http://www.theregister.co.uk/content/28/17700.html>; excerpted by PGN]

---

## 🚀 More on the importance of safeguarding private crypto keys

David Kennedy CISSP <david.kennedy@acm.org>

Tue, 20 Mar 2001 16:08:59 -0500

Cryptologists from Czech company ICZ detected serious security vulnerability of an international magnitude. <http://www.i.cz/en/onas/tisk4.html>

- > A bug has been found in worldwide used security format OpenPGP. The bug
- > can lead to discovery of user's private keys used in digital signature
- > systems. OpenPGP format is widely used in many applications used
- > worldwide, including extremely popular programs like PGP(TM), GNU Privacy
- > Guard, and others. The bug detection comes on the right time, as Philip
- > Zimmermann, the creator of PGP program, has left Network Associates,
- > Inc. and aims to boost OpenPGP format in other products for privacy
- > security on Internet. From the scientific point of view, the discovery
- > goes far beyond actual programs - it has wider theoretical and practical
- > impact.
  
- > A slight modification of the private key file followed by capturing a
- > signed message is enough to break the private key. These tasks can be
- > performed without knowledge of the user's passphrase. After that, a
- > special program can be run on any office PC. Based on the captured
- > message, the program is able to calculate the user's private key in half a
- > second. The attacker can then sign any messages instead of the attacked
- > user. Despite of very quick calculation, the program is based on a
- > special cryptographic know-how.

> Similar vulnerabilities can be expected in other asymmetrical  
> cryptographic systems, including systems based on elliptic  
curves.

DSA and RSA keys are reportedly equally vulnerable.

DMK Comment: A detailed report was supposed to be "released  
shortly" but has  
not appeared so far. The press release does not specify whether  
diddling  
the private key results in any error messages. I hope this does  
not spawn  
another round of "PGP is cracked/cracking/crackable" media  
hysteria. The  
importance of key management has always been critical and this  
would seem to  
only add to the reasons why. There are viruses that try to  
steal PGP's  
secret key, there are trojans that make it possible to steal  
PGP's secret  
key. Storing keys on shared/networked workstations has always  
been  
recognized as a problem with PGP. The comp.security.pgp FAQ  
includes: Can I  
put PGP on a multi-user system like a network or a mainframe?  
<<http://www.uk.pgp.net/pgpnet/pgp-faq/faq-03.html#3.18>>

David Kennedy CISSP, Director of Research Services, TruSecure  
Corp.

<http://www.trusecure.com>

---

## **⚡ Risks of self-induced false alarms**

Graystreak <[wex@media.mit.edu](mailto:wex@media.mit.edu)>

*Thu, 8 Mar 2001 13:57:54 -0500*

<http://washingtonpost.com/wp-dyn/articles/A38625-2001Mar7.html>

FBI Director Louis J. Freeh said he and his wife had been baffled by a series of false alarms from the security system in their Great Falls area home. Fairfax County police responded each time, but no suspects had been nabbed.

It seems that two of his six sons, then ages 5 and 4, had been amusing themselves by making their 2-year-old brother run in circles in the basement to set off the motion detector. "They would sit and watch for the police to come," Freeh said.

[AW notes: no discussion of why the motion detector was on in the basement while the children were home, nor why the police didn't adopt a "call before responding" policy after some number of false alarms.]

---

## **✶ Using automation software without accounting for possible scenarios**

Tony Yip <tonyy@chancery.com>  
Wed, 7 Mar 2001 12:48:36 -0800

>From www.macfixit.com 7 Mar 2001:

Many [Macfixit] readers sent us copies of a letter they received yesterday from the Apple Store apologizing "for the delay in fulfilling" their Mac OS X order. This seemed a bit odd, as Mac OS X won't ship until March 24. So there can be no delay at present. Are they anticipating a delay starting

March 24? Or was the message sent in error, probably as the result of some software that automatically triggered the mailing when it detected that the order had not yet been fulfilled? We suspect the latter, as it makes more sense.

Consistent with our theory, Evan Chaney writes: " I called the Apple Store and talked to a sales rep who said he thinks this e-mail is invalid and that he thinks it was sent just because the system sends out a backlog e-mail if the product hasn't been shipped after 20 days. Apparently, it doesn't account for pre-ordered products." We have no word from Apple on this as yet.

The RISKS: automation is good; but you need to take all scenarios into account; especially when you created the scenario yourself by accepting orders way before the product is due to be shipped.

---

## **✶ Another "secure" e-book seems unlikely**

<risky@moz.net.nz>

*Mon, 12 Mar 2001 18:28:57 -0700*

I just went through an SSL page to purchase an online book from [www.mightybooks.com](http://www.mightybooks.com), with slightly bizarre results. They use the "secure" Acrobat Reader to deliver content, which is a known risk to them (the secure format is anything but).

More concerning is their apparent use of a simple counter in

their download

URL. My URL was of the form:

`https://shop.mightywords.com/servlet/com.mighty.download.`

`HabitatRequestServlet?saleId=xxxx`

where xxxx is a small integer.

Unfortunately I can't test the surmise that trying the next (or prior) few

integers might net me more books, since it requires me to have the 128 bit

encryption "upgrade" installed on Windows 2000 (confusingly, their FAQ

claims that Service Pack 1 will also fix this problem, but I have that

installed). Of more concern is that I could complete the entire sale process

on their secure site, only to fail at the actual download stage because that

requires a higher level encryption than the rest of the sale.

There is no "download a trial document" link on the site (I looked!), so it

seems impossible to verify the problem without actually making a purchase

(or attempting a theft by plugging numbers into the URL above).

Moz

---

## **⚡ The risks of accidentally becoming a customer for life**

Jim Youll <jim@media.mit.edu>

*Thu, 15 Mar 2001 08:50:24 -0500*

In 1998 I helped a company computerize its shipping department.

While

testing documentation and processes, I signed up as a "shipper" in the UPS

online system. I neglected to remove myself when the project was

finished,  
and in 2001, I was still receiving promotional UPS e-mail. The messages do not offer an "unsubscribe" hint.

So I called UPS. "All you need to do," the rep said, "is to go to 'your page' on the Web site, enter the user ID and password, and clear the correct checkbox" to make the e-mail stop. Unfortunately, I didn't know my user ID and password. UPS insisted it had no way to look up an account name if given an e-mail address. They pointed out that it was really my fault for "forgetting" the user ID I created in 1998 and insisted that "clearing the checkbox" was the only way to make the mail stop. Without a user id, there was "no way to get to the checkbox."

After more complaints, they finally contacted the people who run the e-mail database. Turns out I could not possibly have forgotten "the user ID I created in 1998" because in 1998, the system did not employ "user IDs" on accounts -- my records didn't even have one, making them totally inaccessible except to their systems people! Sometime after 1998 the system was changed. UPS says my records are corrected but I don't know if that means I have a "user ID" now, or whether the account was deleted. I wonder about the disposition of the thousands of other early adopters whose accounts lack user IDs.

It's still expensive to use version 1.0, even on the Web.

## **NSF study: "Internet Voting is no 'Magic Ballot'"**

Terry Carroll <carroll@tjc.com>

*Fri, 16 Mar 2001 14:24:58 -0800 (PST)*

RISKS has previously had discussions of the risks associated with going to computerized voting (especially Internet-based voting) as an attempted panacea for the types of problems we saw in the last US presidential election.

The National Science Foundation recently released a study that it commissioned from the Internet Policy Institute on problems associated with Internet voting. The NSF's press release on the study may be found at <<http://www.nsf.gov/od/lpa/news/press/01/pr0118.htm>>. The IPI has a page devoted to the study (including a link to the report itself) at <<http://www.internetpolicy.org/research/results.html>>.

The NSF highlights the following findings with respect to the feasibility of Internet voting:

- Poll site Internet voting systems offer some benefits and could be responsibly deployed within the next several election cycles;
- The next step beyond poll-site voting would be to deploy kiosk voting terminals in non-traditional public voting sites;
- Remote Internet voting systems pose significant risk and should not be used in public elections until substantial technical and social science issues are addressed; and

- Internet-based voter registration poses significant risk to the integrity of the voting process, and should not be implemented for the foreseeable future.

Terry Carroll, Santa Clara, CA <carroll@tjc.com>

[These results are rather similar to the findings of the California commission. Interested readers should also dig up the recent Caltech/MIT report, which states that lever machines, hand-counted paper ballots, and optically scanned ballots are all significantly more accurate than direct-recording voting machines (DREs) and Internet voting schemes. PGN]

---

## ⚡ On line elections

"Sarr Blumson" <sarr.blumson@alum.dartmouth.org>

*Fri, 16 Mar 2001 11:28:20 -0500*

The college I attended is running the election for alumni appointed trustee with a Web voting option through election.com. So I went to cast my vote, and got in response:

Microsoft OLE DB Provider for SQL Server error '80040e14'

The log file for database 'electnet' is full. Back up the transaction

log for the database to free up some log space.

/dartmouth2001/confirmation.asp, line 92

It's happened twice. It let me vote successfully a few hours later; I'm

assuming/hoping it only recorded my vote once.

Not I'm imagining trying to explain to the poll watchers in a real election that this message means they should let me vote again.

Sarr Blumson, JSTOR, University of Michigan, 301 E Liberty, Ann Arbor, MI  
48109-2262 <http://www-personal.umich.edu/~sarr/> +1 734 764 0253

---

## ✶ Smart Bombs - Old Story

"Bruce E. Wampler" <bruce@objectcentral.com>  
*Wed, 07 Mar 2001 14:19:12 -0700*

I've been recently been reading "A War to Be Won: Fighting the Second World War" by Murray and Millet (ISBN 0-674-00163-x), and have gotten a bit of perspective on the RISKS of developing high tech weapons that seems to apply to the recent poor performance of the Navy's Joint Standoff Weapon (smart bomb) in Iraq.

It seems (CNN: <http://www.cnn.com/2001/US/02/26/us.iraq.ap/index.html>) that much of the failure was due to not accounting for high winds, and that a software fix that would have the bombs level off longer might make them work. This is just another example of not finding weapon flaws until they are actually used in the field.

This is, in fact, a very old story. Just one example from "A War To Be Won":  
it seems that the United States submarine fleet was very

ineffective during the first year or more of the Pacific war because of defective torpedoes. The US subs had the latest, high-tech torpedoes available. Fancy magnetic fuses that didn't work, and a faulty guidance system that didn't work either. Turns out, the Navy engineers had tested the torpedoes without a full weight warhead, and so the sensors that measured the water depth were improperly calibrated. Doesn't this sound familiar?

And there are more familiar lessons in the torpedo story. The submarine crews knew the torpedoes didn't work, tried to get the Navy engineers to fix the problem (who denied any problems for a long time) and ended up figuring out how to turn off the magnetic fuses and use a contact fuse (that also had design defects, but worked better anyway), and to field calibrate the depth sensors.

I think these very similar stories - 60 years separated - bring up some interesting points. First, using the latest technology is risky in itself, whether it is new magnetic fuses and depth sensors or satellite guided bombs that fail to account for wind. It will remain impossible to really know how the weapons will work until they are really used. It is not an option to start a conflict just to test the weapons! Second, the engineers will always say their weapons are different, and will work. There are no doubt many more lessons, but for now, a final lesson to remember is that there are really not all that many new RISKS around - it so often comes down to the people involved in using and developing the technology - in 1941 or

2001.

Bruce E. Wampler, Ph.D., [bruce@objectcentral.com](mailto:bruce@objectcentral.com)

---

**✉ Re: Smart bombs miss again (Davis, [RISKS-21.28](#))**

Richard Schroepfel <[rsc@CS.Arizona.EDU](mailto:rsc@CS.Arizona.EDU)>

*Thu, 15 Mar 2001 14:23:50 -0700 (MST)*

For the last century or so, soldiers have been instructed not to take the time to aim their guns: you do more damage by shooting faster.

I don't know what the numbers look like for bombs, but simply knowing "miss/hit" statistics isn't enough information to deprecate the weapon.

Rich Schroepfel    [rsc@cs.arizona.edu](mailto:rsc@cs.arizona.edu)

---

**✉ Re: Smart bombs miss again (Davis, [RISKS-21.28](#))**

"Christophe Augier" <[augier@altran.com](mailto:augier@altran.com)>

*Fri, 16 Mar 2001 12:11:16 -0500*

"Around 50% of smart bomb didn't functioned in the last NATO bombing."

Well, we shouldn't put it this way : 50% of the objectives are still standing. 50% of the enemy facilities, radar, airfields or whatever are still operational. In a "real" war that means retaliation.

Usually, that costs a lot more than a entire load of smart-bombs and their F18.

The risks are not in the bombs malfunctioning, but in the non-realization of the military objectives. If the ponderated (one target may be more important than another) targets destroyed represent, let's say, 65% of the targets, NATO could be satisfied with this objective. It is all relative.

There is another point I wanted to "laser-light" : The cost of the bombing.

Technical risk analysis is ok, but you have to deal with financial risks analysis (e.g. in a long war the risk of issuing money to support the war effort. See Germany in WWI and WWII. ...or the risk of losing your next election because of too much tax money spent :).

Well, you may multiply the % of awaited destroyed targets (they surely have this kind of statistics for all bombs ; let's say 50% for smart bombs? or it could be calculated with the "circular error probable"\*precision of the aim) by the overall costs of the bombing. You will be able to compute the total amount of bombs/money to reach your objectives, and then choose your optimized solution : B52 carpet bombing, smart-bombs, artillery, a mix of them (gulf war), etc.

Of course, all this thinking, does not take in consideration "side effects" as civilian casualties, soldiers/pilots casualties, or destroyed embassies.  
:)

On resume: As we don't know the objectives of the last NATO bombing, nor the

cost of it, I somehow agree with Randy's answer "In the absence of the relevant numbers and relevant comparison points, the widely repeated "more than 50%" is simply meaningless, no matter how melodramatic it sounds."

Christophe

---

## ✶ Re: Smart bombs miss again (Davis, [RISKS-21.27](#))

Pekka Pihlajasaari <Pekka@data.co.za>

*Fri, 16 Mar 2001 07:57:26 +0200*

The original quotation "most of the bombs ... missed their targets." is semantically quite different from "bombs hit fewer than 50% of the targeted radars."

In the original release the military indicated that the majority of their ordnance did not achieve hits. The paraphrasing by Randy changes the semantics to that of a minority of targets did not get hit.

It is quite likely that multiple bombs were targeted at a single radar, and no estimate of the actual number of destroyed targets can be inferred from the original press release. This is assuming that the original release was not equally distorted.

The RISK is that moving even simple sounding numbers out of context can distort the intent of the statement so much as to make it useless. All the

more reason for looking at the source material before drawing a conclusion.

Pekka Pihlajasaari <pekka@data.co.za> Data Abstraction (Pty) Ltd

---

## ✦ Re: Smart bombs miss again (Davis, [RISKS-21.27](#))

Nelson Michael A CNTR AMC/DOTR <MICHEAL.NELSON@SCOTT.AF.MIL>

*Fri, 16 Mar 2001 08:46:06 -0600*

Randy Davis used the term "circular error probable" to describe the accuracy of weapons delivery. That phrase is a cryptic, almost opaque variant of the more intuitive, original terminology "circle of equal probability," and can lead to the casual reader asking two pointed questions:

- \* What exactly is "circular error"?
- \* If something called "circular error" does exist, what meaning does the word "probable" add to the concept?

This entire semantic discussion becomes moot with the use of the original phrase. It captures the underlying concept noted in Mr. Davis' message in a much more meaningful way: for a given weapon system, the circle where, on average, half of the weapons will land inside the circle and half outside the circle. Unfortunately, "circular error probable" is in widespread use, in both technical and non-technical literature.

Michael A. Nelson, Aircrew Force Management Analytical Support  
ARINC, Inc.

**✉ Re: Smart bombs miss again (Davis, [RISKS-21.27](#))**

Bill Stewart <bill.stewart@pobox.com>

*Sat, 17 Mar 2001 12:33:53 -0800*

[...] "One target, one smart bomb" would be fun, but it's unlikely. During the First Gulf War, about 97% of the bombs used were still dumb iron bombs.

Bill Stewart

---

**✉ Re: Smart bombs miss again (Davis, [RISKS-21.27](#))**

(Wm. Randolph Franklin) <rfranklin@altavista.net>

*19 Mar 2001 13:10:51 -0500*

I don't think the bombs were even that accurate until the end of WWII.

There was a British study around 1942 or so that said that most bombs were

more than 5 miles off. IIRC, when Peenemunde was first bombed, the "after"

recon photos looked like the "before" photos.

This illustrates that accuracy can improve.

I have a problem with the argument that something is impossible merely

because it's difficult. This seems to be a proxy for the argument about

whether we should do it, not whether we can do it. There's the joke that

the opponents may be more afraid that it will succeed than that

it will  
fail.

Here's an example of how hard problems sometimes get solved. It's not easy to propel a rocket in a straight line by pushing it from the rear. There is a great movie of NACA and NASA rocket mishaps. It has a rocket making a U-turn immediately after launch (apparently a polarity error in the gyroscope wiring), a rocket lifting off a little, then settling back on the pad, a rocket gently tipping over, etc.

Now, we've solved all that. Launches are 98% reliable.

Perhaps the THAAD is as fundamentally flawed as using a ladder to get to the moon. However, that hasn't been established yet.

(Wm. Randolph Franklin) <rfranklin@altavista.net>



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 21: Issue 29**

**Friday 23 March 2001**

## Contents

- [Identity theft: Forbes-ing a head?](#)
- [Indiana University penetration raises fears of identity theft](#)  
[Keith A Rhodes](#)
- [Serious new CA Drivers License ID RISK](#)  
[Peter V. Cornell](#)
- [Faulty radar prompts FAA inspections and remediations](#)  
[Keith A Rhodes](#)
- [Bogus Microsoft Corporation digital certificates from Verisign](#)  
[Jeff Savit](#)
- [Your PGP E-Hancock can be forged](#)  
[Monty Solomon](#)
- [Czech PGP flaw tech details](#)  
[David Kennedy](#)
- [Politically correct: DoE is slow to warn of computer virus](#)  
[David Farber](#)
- [Nokia cell phone trivially easy to unlock](#)  
[Eric Hanchrow](#)
- [Hacker sentenced to hacking](#)  
[Jeremy Epstein](#)
- [Government, school sites link to porn](#)

[Dave Stringer-Calvert](#)

● [Yahoo! Mail translates attachments](#)

[Matt Curtin](#)

● [Re: Air gaps](#)

[Fred Cohen](#)

● [Re: MIT/Caltech voting study](#)

[Paul Terwilliger](#)

● [German armed forces ban MS software, citing NSA snooping](#)

[Pete McVay](#)

● [MS Word: Ohm, SaveAs Watt](#)

[Kevin Rolph](#)

● [Workshop CFP: Security and Privacy in Digital Rights Management 2001](#)

[Tomas Sander](#)

● [Info on RISKS \(comp.risks\)](#)

---

## ✶ Identity theft: Forbes-ing a head?

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

*Tue, 20 Mar 2001 11:26:58 PST*

In RISKS, we have for many years been warning about the burgeoning increase in identity theft. The following case could foster a broader awareness of the depth of the problem, but then again most folks still seem to have their heads in the sand -- unless they have already been burned.

Abraham Abdallah was arrested on 7 Mar 2001, a 32-year-old Brooklyn NY high-school dropout working as a busboy, and already a convicted swindler.

Although he was arrested as he was picking up equipment for making bogus credit cards, he is suspected of already having stolen millions of dollars.

In his possession were SSNs, addresses, and birthdates of 217

people whose names appeared in a Forbes Magazine itemization of the 400 richest people in the U.S. He reportedly also had over 400 stolen credit-card numbers, and had used computers in his local library to access of the Web for information gathering. He is being held on bail of \$1M. His activities were detected after an e-mail request to transfer \$10M from a Merrill Lynch account, whereupon authorities found mailboxes he had rented in various names and other evidence. His defense attorney said Abdallah is innocent, and that prosecutors had ``made an unfair leap from possession of this information to an inference that there was an attempt to take money.''

[PGN-ed from a variety of sources, including an AP item by Tom Hays <http://www0.mercurycenter.com/premium/business/docs/forbes21.htm>;

Thanks to Dave Stringer-Calvert and to Michael Perkins at Red Herring]

---

## **✶ Indiana University penetration raises fears of identity theft**

"Keith A Rhodes" <RhodesK@GAO.GOV>

*Wed, 28 Feb 2001 10:19:34 -0500*

A user browsing from Sweden stored music and video files on a server at Indiana University that had apparently been left unprotected after a crash. IU realized it had a problem when huge increases were noted in network traffic. In the process, they also noted that a file of over 3,100 student

names and SSNs had been copied from the server. Associate Vice President Perry Metz contacted the Social Security Administration about what might be an appropriate reaction, and said that they told him ``it's unlikely and unusual for someone who has your Social Security number to be able to do anything with it. Normally, financial institutions require additional information.''

[Is that reassuring to RISKS readers? Sources: Swedish hacker breaches IU server; Culprit stored music, video files on system and also downloaded private student data, AP item 28 Feb 2001, and article by John Meunier, \*Herald-Times\*, 28 Feb 2001; PGN-ed]

---

## ✶ Serious new CA Drivers License ID RISK

"Peter V. Cornell" <pcornell@nanospace.com>

*Wed, 21 Mar 2001 16:03:12 -0800*

This is really happening!

Almost exactly one decade ago Chris Hibbert posted a RISKS article describing the (then) new California Drivers License (CDL). He gave a warning to us all. That little piece is still on server:

<http://catless.ncl.ac.uk/Risks/11.03.html#subj10>

[and has been updated by Chris since. PGN]

That warning, given in 1991, has blossomed into a nightmare.

Recently, The California driver license and ID card have been declared as PRIMARY IDENTIFICATION DOCUMENTS in this state by the California

legislature.

<http://www.dmv.ca.gov/faq/dlfaq.htm#2504>

<http://www.lbl.gov/Workplace/HumanResources/irss/dmv.html>

Guess why? A great convenience for bankers, but enabling serious new ID fraud RISKS based on easily obtained fake driver licenses and data.

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

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

<http://www.wdia.com/home-entrypage.htm>

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

Courtesy of the California legislature, \*anyone\* who has a fake California drivers license with YOUR correct data, but with \*his\* picture and \*his\* version of your signature, can steal your money in many different ways. For example, if he knows your Social Security Number, bank, and account number, (easily obtained online or by mail theft) he can walk into any branch office and receive cash. Tens of thousands have been stolen from my (no longer existent) Wells Fargo accounts.

I must be one of the very first victims of this new kind of identity theft. I have been scouring the internet for months and have found no mention of it. Of course there are gigabytes of stuff about the old credit card scams, alive and still growing, but no mention of use of drivers licenses to impersonate bank customers and withdraw cash directly.

With that fake drivers license, that fraudster becomes YOU. All he need do

is write a bad check drawn on another bank's bogus name account set up for that purpose, with the victim (you) as payee. He then walks into (in my case) a Wells Fargo branch and, impersonating the victim, cashes the check. When the check bounces, Wells Fargo (probably others, too) simply debits the victims account.

The banking industry has arranged the law (California Commercial Code Sections 4401-4407 and 3101-3119) to ensure that the customer takes the hit. So that, among other conveniences, THE LAW allows banks to rely \*solely\* on the CDL data to confirm the identity of a customer with no risk exposure whatsoever. "IF THE CUSTOMER PROVES" means you must sue the bank. They have it written so you'd lose anyway, but the amounts, however painful, are not nearly enough to pay a lawyer. (See excerpts from the California Commercial Code below.)

So, with my CDL data in circulation, if I want to keep a checking account, I must change banks regularly. There are at least two fraud artists still using my ID.

The banks DO check your CDL number as well as date of birth at the teller window. But there is no possible way to change any of my drivers license data. The California Department of Motor Vehicles (DMV) web site says to go to a local office to change your drivers license number. That just plain doesn't work. Many of the items on their ID Theft page simply do not work in actual practice. It \*looks\* pretty.

<http://caag.state.ca.us/identity.htm>

The DMV local says they'll replace your picture ID with one that has no picture while your request is being processed which may take months. Impossible! They also require a letter from the bank. But none of the Wells Fargo's "headsets" (customer service phone reps) or "robots" (branch employees) are able or willing to do that. They'll give you forms to fill out which are totally inadequate for this new kind of ID fraud. Bank customers are thus denied any access to the bank officers responsible and accountable for bank policy.

Bankers have their political money well spent. With their credit cards, computers, headsets and robots, their ethics, "good faith" and accountability were abandoned long ago.

Peter V Cornell <pcornell@nanospace.com>

- - - -

CALIFORNIA CODES COMMERCIAL CODE SECTION 4406 [excerpted]

(d) (2) The customer's unauthorized signature or alteration by the same wrongdoer on ANY OTHER ITEM paid in good faith by the bank if the payment was made before the bank received notice from the customer of the unauthorized signature or alteration and after the customer had been afforded a reasonable period of time, NOT EXCEEDING 30 DAYS, in which to examine the item or statement of account and notify the bank.

(e) If subdivision (d) applies and the CUSTOMER PROVES that the bank failed to exercise ORDINARY CARE in paying the item and that the failure

contributed to loss, the loss is allocated between the customer precluded and the bank asserting the preclusion according to the extent to which the failure of the customer to comply with subdivision (c) and the failure of the bank to exercise ORDINARY CARE contributed to the loss. IF THE CUSTOMER PROVES that the bank did not pay the item in good faith, the preclusion under subdivision (d) does not apply.

CALIFORNIA CODES COMMERCIAL CODE SECTION 3103.

(a) (7) ORDINARY CARE "... in the case of a bank that takes an instrument for processing for collection or payment by automated means, reasonable commercial standards DO NOT REQUIRE THE BANK TO EXAMINE THE INSTRUMENT..."

(To see the complete text of the above California Commercial Code Sections, go to <http://www.leginfo.ca.gov/calaw.html> Check the "Commercial Code" box, enter keyword "4401", then click search.)

---

## **✶ Faulty radar prompts FAA inspections and remediations**

"Keith A Rhodes" <RhodesK@GAO.GOV>

*Mon, 19 Mar 2001 07:32:49 -0500*

The ASR-9 radar system in use at 134 major U.S. commercial and military airports has recently had some serious mechanical failures -- notably in Boston on 22 Apr 2000 and NY's JFK on 17 Dec 2000. The Federal Aviation Administration ordered an inspection, which detected 23 further

cases of similar problems. 17 had the same problem that Boston had -- stripped rivets in the support assembly. The other 6 had the JFK problem -- a stripped jackscrew assembly for positioning the antenna. Various remedial actions are underway to hopefully prevent future collapses, with an estimated total cost of \$22 million. [Source: Problems at 23 Installations Are Linked to Support Stands or Tilt Mechanisms, Don Phillips, \*The Washington Post\*, 19 Mar 2001, A02; PGN-ed]  
<http://www.washingtonpost.com/wp-dyn/articles/A23566-2001Mar18.html>

---

## ⚡ **Bogus Microsoft Corporation digital certificates from Verisign**

Jeff Savit <Jeff.Savit@Sun.COM>  
*Thu, 22 Mar 2001 17:12:06 -0500*

Spoofing hazard: Verisign gave digital certificates under Microsoft name to an individual not from Microsoft. Microsoft issued a bulletin at <http://www.microsoft.com/technet/security/bulletin/MS01-017.asp> that describes the risk of running code that erroneously appears to be signed by Microsoft (eg: ActiveX controls), and discusses the risks due to not having a proper revocation mechanism.

Note that the certs were made available January 30th, so who knows what code has been accepted and executed since then. Microsoft is a victim in this particular instance.

Jeff Savit, Sun Microsystems 1-201/498-8306 Jeff.Savit@sun.com

[Noted by quite a few RISKS contributors. Many thanks! PGN]

---

## **⚡ Your PGP E-Hancock can be forged**

Monty Solomon <monty@roscom.com>

*Wed, 21 Mar 2001 17:09:00 -0500*

A Czech information security firm has found a flaw in Pretty Good Privacy that permits digital signatures to be forged in some situations. Phil Zimmermann, the PGP inventor who's now the director of the OpenPGP Consortium, said that he and a Network Associates (NETA) engineer verified that the vulnerability exists.

<http://www.wired.com/news/politics/0,1283,42553,00.html>

---

## **⚡ Czech PGP flaw tech details**

David Kennedy CISSP <david.kennedy@acm.org>

*Thu, 22 Mar 2001 18:23:24 -0500*

The promised technical paper is at:

[http://www.i.cz/en/pdf/openPGP\\_attack\\_ENGvktr.pdf](http://www.i.cz/en/pdf/openPGP_attack_ENGvktr.pdf) (PDF, 100 KB)

"The attack to private signature keys in OpenPGP format, PGPTM program and other OpenPGP based applications" here.

[http://www.i.cz/pdf/pgp/OpenPGP\\_Attack\\_ENGfinal.ppt](http://www.i.cz/pdf/pgp/OpenPGP_Attack_ENGfinal.ppt) (PPT, 81 kB)

ICZ's scientists' reactions to criticism and FAQ

<http://www.i.cz/en/onas/ohlasy.html>

[...]

Hal Finney has a succinct analysis posted to the Open-PGP list archived at:

<http://www.imc.org/ietf-openpgp/mail-archive/msg04767.html>

My summary of Hal's analysis:

1. Attackers have to diddle the secret key.
2. Does *\*not\** work with commercial PGP 7.0.3 w/RSA keys (unknown about earlier).
3. Does work with all DSA keys and RSA keys in GPG.

Dave Kennedy CISSP Director of Research Services TruSecure Corp.

<http://www.trusecure.com>

[Debate rages over whether this is a realistic attack. Once again, the vulnerability of underlying operating systems and the presence of subvertible networked resources makes such attacks easier. PGN]

---

## **✶ Politically correct: DoE is slow to warn of computer virus**

David Farber <dave@farber.net>

*Sun, 18 Mar 2001 9:36:24 PST*

The "Naked Wife" virus was already wreaking havoc, but when DoE headquarters set out to warn the troops, the politically correct DoE

software balked at the word "naked." WN has been told that it took

several hours before the warning could be passed on.

[From Dave's IP. For archives, see: <http://www.interesting->

[people.org/\]](http://people.org/)

---

## **✶ Nokia cell phone trivially easy to unlock**

Eric Hanchrow <offby1@blarg.net>

*20 Mar 2001 10:04:50 -0800*

My cell phone -- a Nokia 8260 -- has lots of information in it that I wouldn't want divulged. Examples: phone numbers of friends, my calling-card number, a detailed record of all the calls, text messages, and e-mail messages that I've made or received. And, of course, I certainly wouldn't want anyone who got hold of my phone to be able to place calls with it, thus forcing me to pay for them.

Until recently, I assumed that the phone's "lock" feature would indeed protect the information and prevent unauthorized use. However, I now believe that that feature is close to worthless.

Here's how it's supposed to work:

The phone stores two secret numbers, which act essentially as keys. One number, called the "security code", is like a master key, in that if you know this number, you don't need the other; the other, called the "lock code", is like a regular key. You can set the phone up to "lock" itself as soon as you turn it off. This means that, the next time you turn it on, the phone will be unable to place calls until you enter the lock

code. Thus the lock code appears to protect the information -- you can't poke around in the phone's menu system to read the information while the phone is locked -- and to protect against unauthorized use, since you can't place calls while the phone is locked.

Now, there's a handy feature built into the phone that will save you if you've forgotten the lock code, but still remember the security code: merely enter the wrong lock code five times in a row, and the phone will then ask for the security code. Once you enter the security code, the phone unlocks, and you can then change the lock code to something you will remember. So if you know the security code, you don't need the lock code.

Surely, you can see where I'm headed: I've discovered that it's trivially easy to find out the phone's security code, even if you don't know the lock code, even if the phone is locked. All you need to do is turn the phone on, enter a magic string of digits and symbols (which I won't divulge here, but which is *\*very easy\** to find on the web), and then scroll through an undocumented menu hierarchy until you find a menu called "security". Once you select that menu, the phone displays its security code. You then turn the phone off and on, enter the wrong lock code five times in a row, enter the security code when prompted, and the phone is now yours.

---

## Hacker sentenced to hacking

"Jeremy Epstein" <jepstein@webmethods.com>

*Fri, 16 Mar 2001 15:48:46 -0500*

A teenager who was convicted of defacing Web sites must serve a sentence that includes programming the jail's computers (see <http://www.usatoday.com/life/cyber/tech/2001-03-09-coolio.htm>). Talk about putting the fox in charge of the henhouse! What's going to happen when he puts in some backdoors to change the behavior of the system to better suit his needs? Who will be able to correct the problems introduced this way?

--Jeremy

[We noted a case 15 years ago of a prisoner gaining access to the prison information system to change his release date, plus three cases of bogus release messages. PGN]

---

## **✶ Government, school sites link to porn**

Dave Stringer-Calvert <dave\_sc@csl.sri.com>

*Fri, 23 Mar 2001 08:42:19 -0800*

Farmers and gardeners around the country looking for growing tips from university research centers are currently being pointed to pornography instead. Hundreds of university and government Web sites including the U.S. Department of Agriculture are linking to the porn site, which has taken

over the domain of an important agricultural resource center. The university that runs the site blames bad record keeping at Network Solutions, which maintains part of the Internet's domain names system.

<http://www.msnbc.com/news/547652.asp>

---

## **✶ Yahoo! Mail translates attachments (Re: Frankston: RISKS-21.27)**

Matt Curtin <cmcurtin@interhack.net>  
16 Mar 2001 09:59:23 -0500

> <http://www.zdnet.com/zdhelp/stories/main/0,5594,2631218,00.html>

Unfortunately, ZDNet has chosen not to put its story on a single page; the two paragraphs at the cited URL are just the introduction; one must click through the rest of the story. Therein, we learn what's happening.

One example of translation is instances of "expression" being changed to "statement". It appears that the translation -- RISKy as it could be -- is itself a "feature" to minimize risk. Namely, the risk of malicious JavaScript or ActiveX code.

There are a lot of issues raised by this; unfortunately none of the raised issues is new. It's not hard to argue that using the web (built atop the stateless protocol HTTP, rife with lots of potential for leaky channels of

communication and therefore privacy problems) for email is the Wrong Thing to do.

It seems to me that translation of words that could potentially be read by an eager JavaScript interpreter fails to follow mom's maxim: two wrongs don't make a right.

Matt Curtin, Founder Interhack Corporation <http://www.interhack.net/>

---

## ✉ Re: Air gaps (Jaffe, [RISKS-21.27](#))

Fred Cohen <fc@all.net>

*Fri, 16 Mar 2001 06:50:48 -0800 (PST)*

It's hard to believe that people in the 'security business' who have claims that are so unworthy of trust can continue to exist.

Of course all systems have covert channels - after all, it is the wave nature of matter and energy - and yet an air gap is supposed to mean that there is literally no connection between the components other than the one afforded by subatomic forces acting over a distance across the 'air gap'. The distance across of the air gap then leads to the signal strength across the distance and we can calculate how far away things need to be to have very nearly zero chance of passing a digital level signal.

But the term "air gap" is fraudulent as used in these product claims. That

are nothing like air gaps. They are in fact directly connected systems with wires between them and no air gap at all.

Being able to remotely send an email that causes the introduction of software that gets into the 'inside' and sends results back to the 'outside', even if not instantaneously.

Is very very different from

Being able to induce current in a proximate system by getting close enough to it to create the proper fields and having a sensitive enough specialized piece of electronics gear there to detect the changes in signal strength returning from the other side.

Mr. Jaffe may wish to minimize this difference through rhetoric, but I do not think it is accurate to do so.

Fred Cohen at Sandia National Laboratories at tel:925-294-2087  
fax:925-294-1225

Fred Cohen & Associates: <http://all.net> - fc@all.net - tel/  
fax:925-454-0171

Fred Cohen - Practitioner in Residence - The University of New Haven

---

## ✶ Re: MIT/Caltech voting study (PGN, [RISKS-21.28](#))

Paul Terwilliger <pault@gsinet.net>  
*Wed, 21 Mar 2001 20:06:21 -0500*

In [RISKS-21.28](#), PGN commented after a writeup about the NSF study of internet voting:

> [These results are rather similar to the findings of the  
California  
> commission. Interested readers should also dig up the  
recent Caltech/MIT  
> report, which states that lever machines, hand-counted paper  
ballots, and  
> optically scanned ballots are all significantly more  
accurate than  
> direct-recording voting machines (DREs) and Internet voting  
schemes. PGN]

The MIT/Caltech voting technology project's \*preliminary\*  
report, available  
at <http://www.vote.caltech.edu/Reports/report1.pdf>, studies the  
"residual  
vote", which is defined in this context as the difference  
between the number  
of voters who sign-in (the turnout), and the total votes cast  
for president.

This report did indeed conclude that lever machines and hand-  
counted ballot  
jurisdictions had the lowest average residual vote (1.8% and  
2.0%,  
respectively), and DRE (3.0%) one of the highest. Internet  
voting was not  
studied.

Are the differences statistically significant? I do not know.

Are there external factors at work? It would seem likely.  
Ballot design  
can be logical or confusing - doesn't matter what type of  
technology is  
being used! Introduction of new systems may cause confusion.  
Heavy turnout  
and long lines may cause voters to walk out after signing in.

Or there could be problems with a particular system or  
technology.

However, it is a long stretch to take the conclusions of this

study and make claims that one system is "significantly more accurate" than another.

Paul Terwilliger, Sequoia Voting Systems

---

## **German armed forces ban MS software, citing NSA snooping**

"Pete McVay" <pmcvay@tiac.net>

*Mon, 19 Mar 2001 05:58:36 -0500*

The German foreign office and Bundeswehr are pulling the plugs on Microsoft software, citing security concerns, according to the German news magazine

*\*Der Spiegel\**, which claims that German security authorities suspect that the US National Security Agency (NSA) has 'back door' access to Microsoft

source code, and can therefore easily read the Federal Republic's deepest secrets. The Bundeswehr will no longer use American software (we surmise this includes Larry and Scott as well) on computers used in sensitive areas.

The German foreign office has meanwhile put plans for videoconferencing with its overseas embassies on hold, for similar reasons.

Undersecretary of State Gunter Pleuger is said by *\*Der Spiegel\** to have discovered that "for technical reasons" the satellite service that was to be used was routed via Denver, Colorado.

According to a colleague of Pleuger, this meant that the German foreign services "might as well hold our conferences directly in Langley." We're not

entirely sure whose interesting video conferencing via satellite service has a vital groundstation in Denver, but we note that Pleuger seems to have gleaned this information from a presentation held earlier this month in Berlin by, er, Deutsche Telekom. Which just happens, along with Siemens, to have picked up the gig. The two companies have supplanted Microsoft (and anything else American) and will be producing a secure, home-grown system that the German military can be confident in.

[From an article by John Lettice in *\*The Register\**, 17 Mar 2001, German armed forces ban MS software, citing NSA snooping <http://www.theregister.co.uk/content/4/17679.html>]

---

## ⚡ MS Word: Ohm, SaveAs Watt

Kevin Rolph <kevin@kgames.demon.co.uk>  
*Wed, 21 Mar 2001 21:38:03 +0000*

Reviewing an intranet document the other day, I was puzzled to see electrical resistances given in kilowatts!

I'd created the document from a Word document using save-as HTML and it had automagically converted the Omega symbols into 'W's (and not to mention 'tick's into 'v's).

I recall seeing a passing generic warning about symbols but as I had used a club / clover-leaf symbol as a marker elsewhere I'd assumed it meant that.

It didn't actually say \*which\* symbols it was bothered about.

Kevin Rolph, Cambridge, UK

[Thanks for that one. It is a real joule. How about  
omegawatts? PGN]

---

## **✶ Workshop CfP: Security and Privacy in Digital Rights Management 2001**

Tomas Sander <sander@intertrust.com>

*Thu, 15 Mar 2001 15:39:33 -0800*

[Excerpted for RISKS. Looks like a really interesting  
workshop.

For full CfP see the workshop Web site:

<http://www.star-lab.com/sander/spdrm/>

PGN]

### CALL FOR PAPERS

WORKSHOP ON SECURITY AND PRIVACY IN DIGITAL RIGHTS MANAGEMENT  
2001

Philadelphia, Pennsylvania, USA, 5 November 2001

held as part of the Eighth ACM Conference on Computer and  
Communications Security (CCS-8)

This workshop will consider technical problems faced by rights  
holders (who seek to protect their intellectual property rights) and end  
consumers (who seek to protect their privacy and to preserve access they now  
enjoy in traditional media under existing copyright law). Submissions  
are due

3 Aug 2001. Program Chair Tomas Sander, InterTrust STAR Lab,  
sander@intertrust.com, +1-408-855 0242



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 21: Issue 30**

**Monday 26 March 2001**

## Contents

- [Electronic tax filing problems blamed on 'user error'](#)  
[PGN](#)
- [Cyber surfers caught by fishing nets](#)  
[Tin Tin](#)
- [RISKS of rodent teeth](#)  
[Gregory Soo](#)
- [Identity Theft -- a personal experience](#)  
[name withheld](#)
- [Re: California Drivers License as ID for banks](#)  
[John McCalpin](#)
- [Re: "Internet Voting is no 'Magic Ballot'"](#)  
[Douglas W. Jones](#)
- [Verisign certificates problem](#)  
[Roy Sinclair](#)
- [When security is based on trust](#)  
[Michael Sinz](#)
- [Re: Aasta train crash ... safety-critical error](#)  
[Tor-Einar Jarnbjo](#)  
[Dave Aronson](#)
- [IEEE \\*Software\\* Special Issue on Building Software Securely](#)

[Anup Ghosh](#)

● [Info on RISKS \(comp.risks\)](#)

---

## ⚡ **Electronic tax filing problems blamed on 'user error'**

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

*Fri, 23 Mar 2001 16:18:47 PST*

Thousands of electronically filed tax forms are being rejected by the IRS. Apparently that new software may be to blame. The new system requires a five-digit PIN (which is used as ``an electronic signature'!!!!). Taxpayers are also required to provide the adjusted gross income and total tax from the previous year's filing. As a result, Intuit and H&R Block are both reporting 20% rejection rates on electronic returns, blamed on ``user confusion'. The IRS expects 42 million electronic returns this year -- 70% of all returns. [Source: an UNDATED item at cnn.com somewhen earlier in March 2001; PGN-ed.]

[Typo in March date fixed in archive copy.

Added note: The 70% figure seems BOGUS. PGN]

---

## ⚡ **Cyber surfers caught by fishing nets**

Tin Tin <onuj23@juno.com>

*Thu, 22 Mar 2001 15:20:56 -0800*

From : <http://www.theaustralian.com.au/>

Cyber surfers caught by fishing nets, AFP, 22 Mar 2001

China's Internet links with the US are threatened by the anchor nets used by the country's fishing industry. \*The Shanghai Daily\* reported on 21 Mar 2001 that fishing equipment had snagged underwater cables off the coast of Shanghai three times in the past two months, causing havoc for millions of Net surfers. And officials fear the problem could worsen, the paper said. China's main fishing season has just begun and industry officials say they lack sufficient legal power to stop further damage, the report added.

The problem centres on a type of fishing net developed in South Korea that uses anchors sunk into the seabed. Strong tides can drag the anchors -- which are sunk lower into the seabed than Internet cables, for distances of up to 8km -- severing communications links.

Anchor nets are due to be phased out by 2006, but China's Ministry of the Information Industry and the Ministry of Agriculture, which regulate the Internet and fishing industry, are still working on an interim solution. For the next three months, however, authorities in Shanghai can do little but increase patrol boats in the cable areas to warn fishermen away, and industry officials warn that may not be sufficient to prevent a severe breakdown in communications.

The first serious break occurred on 9 Feb 2001 about 370km off China's coast, severing the main Internet link between China and the

US. Although communications were partially restored during a repair process that stretched over two weeks, 22.5 million customers, including many in Shanghai, suffered slow service, the paper reported. On 9 Mar, the Internet backbone linking Taiwan and Shanghai was cut by a fishing net about 120km south of the city, affecting four million users.

When that split was finally repaired on 19 Mar, authorities found another break in the undersea cable that will disrupt Internet services for a further two weeks. Each break costs about six million UN (\$1.4 million) to repair, in addition to unknown business losses resulting from the Internet disruptions.

---

## ✂ **RISKS of rodent teeth (Re: Soo, [RISKS-21.27](#))**

"Gregory Soo hotmail" <grsoo@hotmail.com>  
*Sat, 24 Mar 2001 18:08:55 -0500*

The saga continues strangely: a rodent chewed through cable that had been exposed while Canadian National Railway workers were repairing the cut caused by the would-be copper thieves (noted in [RISKS-21.27](#)). This disrupted service to about 300,000 customers in Ontario's Niagara region, including Sprint Canada and AT&T.

[Source: Animal takes byte out of Rogers, Steve Erwin, The Canadian Press,

24 Mar 2001 <http://www.ottawacitizen.com/hightech/010324/5060312.html>]

---

## **Identity Theft -- a personal experience (from IP)**

<[Identity withheld]>

*Mon, 26 Mar 2001 13:53:40 -0500*

[Contributed by an unidentified individual to Dave Farber's IP list,

For IP archives see: <http://www.interesting-people.org/> .  
PGN]

The following happened to a colleague. About a year ago he signed up for a membership at a video rental store. The form had a place for social security number and he made the mistake of filling it in. About three months later there was a message on his answerer from a bank with which he did not have an account asking about an overdraft. Upon calling he discovered that there was an account in his name with his ss number but with a different address. On calling and writing to the various credit bureaus, he discovered that there had been numerous queries about his creditworthiness. He then contacted each of these and discovered that there had been many credit cards issued in his name as well as a variety of wireless phone accounts. He called each of these in turn and got letters from the credit bureaus but could not be sure that the matter had ended.

The accounts/credit cards were in states other than his but

police in those communities were not responsive to complaints. Fortunately, a friend worked in a state attorney general office and he made a call to a local official in the area where the perpetrators seemed to be based. In addition, quite by accident a local house was raided for drugs. Fortunately, one of the police in the raid remembered my colleague's name so when they discovered a collection of driver's licenses from a variety of states, as well as credit cards and other account info, in my colleague's name, he was able to put it all together. There were also cards and licenses for others. The perpetrators pled and got some jail time... probably more because of the drugs than the identity thefts and fraud.

All of this involved an incredible number of hours and associated aggravation to track down and fix the problem. And resolving it quickly depended on having a well placed connection and a good deal of luck.

The lesson is that we are all vulnerable. Just a ss number is enough to get a fraud going. AND There is no privacy wrt ss numbers. For example, at many universities the ss number is the same as the student ID...and appears on class rosters sent to departments and faculty.

---

**✶ Re: California Drivers License as ID for banks (Cornell, [RISKS-21.29](#))**

John McCalpin <mccalpin@austin.ibm.com>

*Fri, 23 Mar 2001 15:22:06 -0600*

There is nothing new about this scam -- the new law just allows the bank to disclaim financial responsibility for the loss.

I was hit by this exact scam in Texas in 1979. After some telephone calls, the bank covered the loss and I never heard about it again. I am not surprised that the banking industry would make an effort to get legal protection so they could share the pain.

For those inclined to law-breaking, this scam seems like a really easy way to steal money....

John D. McCalpin, Ph.D.  
Senior Scientist

mccalpin@austin.ibm.com  
IBM POWER Microprocessor Development

---

## **✶ Re: "Internet Voting is no 'Magic Ballot'"**

"Douglas W. Jones" <jones@cinnabar.cs.uiowa.edu>  
*Wed, 21 Mar 2001 15:31:22 -0600*

First, I wish people would stop talking about Internet voting as if it was a completely different animal. It isn't. Traditional absentee voting and vote by mail are also done from the home, raising problems of difficult voter authentication and insecure ballot transmission. Direct recording voting machines and precinct-count mark-sense and punched-card ballot systems also use computers and many now offer transmission of

totals over  
public telecommunications systems (frequently phone and radio).  
We should  
address these risks across the board! The way things are going,  
I'm afraid  
we'll end up quite properly stamping out the threat of immediate  
Internet  
voting while leaving the significant flaws of these other voting  
systems  
largely un-addressed!

We should treat Internet voting as direct recording absentee  
voting using  
electronic communication of ballots and vote totals, and we  
should address  
the threats it raises by fixing the laws regarding absentee  
voting, direct  
recording voting systems and use of electronic communication in  
elections!  
Yes, the Internet does introduce some new problems, but these  
other problems  
are far, far broader!

Second, I have been involved with certification testing of DRE  
machines, and  
I've found that it is extremely difficult! With mark-sense and  
punched card  
systems, you prepare a test deck or a test ballot stack, and  
then run those  
ballots through the system, checking to see that the totals  
reflect your  
test. You can hand-count your test deck and arrange all the  
votes to come  
up in easy to recognize patterns in the final total.

In contract, with DRE systems, you have to stand there in front  
of the  
machine doing a repetitive and mind-numbing exercise, entering  
ballot after  
ballot into the machine. After a few ballots, your mind begins  
to wander.  
After a few tens of ballots, your fingers are sore from pushing  
buttons or

tapping the screen, and by the end of your test, you've made so many mistakes that the numbers are meaningless.

A voter casts only one ballot, and for the voter, the voting experience is a peak moment. I've concluded that DRE machines are extremely difficult to test because of this! Hundreds of volunteers (or paid experimental subjects) might be able to run a good test, but even then, they'd be required to vote from a sheet of paper instructing them what candidates to select in order to follow the test plan. Alternatively, the hundreds of voters could be closely observed (perhaps by discretely hidden video cameras), in order to observe how they vote and then compare this to the election result.

The FEC's "voluntary" standards suggest a button-pushing robot to perform such tests, but for accurate testing, this would need a functioning vision system so it reacts to the feedback provided by the machine.

In sum, I've concluded that the accuracy of DRE machines is extremely hard to assess -- so much so that I don't see any reason to trust the assessments that have been made, whether they're positive or negative!

Douglas W. Jones <jones@cs.uiowa.edu>

---

## Verisign certificates problem

"Sinclair, Roy" <RCSinclair@CESSNA.TEXTRON.COM>

*Fri, 23 Mar 2001 09:30:54 -0600*

[From BUGTRAQ@SECURITYFOCUS.COM,  
Via both Mike Hogsett and Dave Stringer-Calvert. TNX. PGN]

Some information regarding Verisign Certificates that has come out of this fiasco is quite disturbing but has been under reported and may have been missed by many in the security business.

Pay close attention to this paragraph from the Frequently Asked Questions part of <http://www.microsoft.com/technet/security/bulletin/MS01-017.asp>:

"The update is needed because of a characteristic of VeriSign code-signing certificates. Every certificate issuer periodically generates a Certificate Revocation List (CRL), which lists all the certificates that should be considered invalid. A field in every certificate should indicate the CRL Distribution Point (CDP) - the location from which the CRL can be obtained. The problem is that VeriSign code-signing certificates leave the CDP information blank. As a result, even though VeriSign has added these two certificates to its current CRL, it's not possible for systems to automatically download and check it. "

The first question I have after seeing that is how many of the rest of the 500,000 certificates that Verisign says they have issued also do not have this CRL Distribution Point field properly filled in. In the lack of any information to the contrary I would hazard to guess that it's probably that none of the 500,000 certificates issued by Verisign have supplied the

information that should be in this field. If this is truly the case then we have yet another problem of much wider scope than the improper issuance of two certificates, there are a great number of valid certificates which could be stolen or misused and even if Verisign were to add them to their CRL the certificates themselves don't point to the CRL so they won't be properly rejected.

Two things need to be done, one is that software which checks certificates must be changed to warn users that certificates lacking a CRL are much more suspect and Verisign needs to re-place all certificates that currently lack this critical information with new certificates that have this field properly filled in. Additional questions that come to mind is how many other certifying agencies have also failed to fill in the information in this field and what percentage of the certificates being used today are unverifiable?

---

## **✶ When security is based on trust**

Michael Sinz <Michael.Sinz@sinz.org>

*Thu, 22 Mar 2001 15:30:32 -0500*

So, lets see - Microsoft says that ActiveX is secure as long as the software (ActiveX thing) is not from an "evil" source. To prevent bad software from being used, they use digital signatures to identify the person or company who made the software such that you could either trust them or know who to

go after when it does something bad. The OS and system infrastructure does not try to enforce anything other than to check these certificates and warn you based on your settings as to if you want to run unsigned software or any software signed by company "X" or a number of other possible combinations of warnings.

There is no built in security beyond that point. Once you say "Yes, run it" you are opening up your system to complete control by the ActiveX control.

Ok, in a perfect world, with no one wishing to do harm or rob you blind, such a mechanism would work just fine. The Internet is not such a world.

And now, to put this into even brighter "this is not the right way to do things" light, Microsoft says that you can not even trust that software that says it is from Microsoft really is from Microsoft unless you first check the dates on the digital signature and remember that if it is Jan 29 or 30, 2001, that it is most likely not really Microsoft and you should not accept it.

What do people do now? If you accept anything from Microsoft, it is too late. If you ask for confirmation before running, what are the chances you would even think to look at the dates once you see "Microsoft" as the signing party?

All of this really goes to show that security must be done at the start and not just "added in" by saying "make sure you trust the author".

Even if you trust the author, there could be bugs. And, as this example shows, you can not even always trust you know who the author is.

Time to think this though some more...

<http://www.zdnet.com/zdnn/stories/news/0,4586,5079987,00.html?chkpt=zdhpnews01>

---

## **✶ Re: Aasta train crash ... safety-critical error (Setzer, [RISKS-21.28](#))**

Tor-Einar Jarnbjo <Tor-Einar.Jarnbjo@pobox.com>  
*Fri, 23 Mar 2001 04:39:34 +0100*

As Anton Setzer is speculating about certain things which obviously are discussed only in the Norwegian part of the report, I think I will be able to clarify a few points and bring some details not mentioned by him.

Actually, the train-controlling system warned only about a malfunction of the set of points at the northern exit of Rustad station, caused by the northbound train forcing it open when driving out of the station. The warning was issued as a static text line with 16mm (0.6") high red letters at the bottom of the monitor. There was no sound signal or flashing light/text to get the train controller's attention. The warning was issued at 13:09:28 and as he was currently occupied with another train line displayed on another monitor, he didn't notice the situation

before some  
time between 13:10:54 and 13:11:58. The report states, that the  
train  
controller can not be held responsible for overseeing the  
warning for 90-150  
seconds.

The mobile-phone numbers had been reported by both train drivers  
to the  
train-controlling central, but the train controller on duty  
earlier the same  
day hadn't written down the numbers where he was supposed to. It  
was also a  
relatively new situation that the phone numbers had to be  
reported to the  
train controlling central. Up until a few months before the  
accident, the  
railway company had been using a UPT service (like British 0700-  
numbers)  
making it possible to call a train using a (fictive) number like  
0700 123  
<train number>. As this service had been canceled by the  
operator Telenor,  
all train drivers had to call the train controlling central and  
report their  
train number and the corresponding mobile phone number.

The report states that it is highly unlikely that the exit  
signal for the  
northbound train was green, but it might have happened, that  
either the red  
signal disappeared (no signal showing) or that it switched to  
green for 3-5  
seconds. The reason for this is, that the security system in  
NSB87 which is  
supposed to make it impossible for the train controller to issue  
a green  
signal on both sides of a track segment operates independent of  
the main  
system and may actually take a few seconds to "discover" the  
failure and  
then do something about it. The older NSI63 signalling system  
operates with

mechanical safety relays which should make it physically impossible, that a green signal is shown on both sides of a track segment. But, there are no commands logged from the train controller where he tries to issue a green signal to the northbound train, and there is no reason to assume that the exit signal switched to green and was corrected by the security system.

The northbound train started according to the train's "black box" 13:07:17 and passed exit signal according to the train control central log 13:07:58. Time enough for the train driver to notice that the signal had switched back to red.

To clarify the situation a little bit:

The accident happened between Rustad station (on the south side) and Rena station (on the north side). The two trains were supposed to cross at Rustad station, but it is discussed in the report if it is likely to believe that the train driver of the northbound train had reason to believe that the crossing had been moved to Rena station. The southbound train was already delayed and the northbound train would also have been delayed if it was supposed to wait for the southbound train at Rustad. But, the train controller had decided to let the trains cross at Rustad as planned, since a crossing at Rena would have caused further delay to the southbound train and also would have caused a connecting train from Hamar to Oslo to be delayed. It is also thoroughly discussed and concluded that neither the driver nor the conductor of the northbound train could have been

aware that  
the southbound train was delayed by about 10 minutes.

But, as the report states, the train driver of the northbound train seemed to suppose that the crossing was moved to Rena for the following reasons:

\* When stopping at Rustad, he did not drive far enough into the station area to let a crossing train drive through the station. Because he stopped the train so far south, the main track behind him had not yet been "cleared" and the south exit signal of the crossing track showed red.

\* The train log shows sign of the train driver being "in a hurry". He held a higher speed than normal when approaching the station, and the train normally only stops at the station "on demand". It is clear that noone left the train at Rustad station, and the train driver might have been prepared to drive through without stopping if it had not been for a passenger waiting for the train at the station.

\* The train left Rustad 13:07:17 after a halt of only 15-20 seconds, although it according to the time table is not supposed to leave until 13:10. The train driver was known to be a very correct person and his watch was found after the accident still going, only 12 seconds off correct time.

>- It might be that a train drives over a red light while running. In the  
> situation in question however, the local train was waiting at a station,  
> and when waiting in front of a red light, it is unlikely to

drive over it.

That is also what the report concludes. It might happen that a train driver oversees a red signal from a running train, but it is extremely unlikely that a train driver on purpose starts from a station and passes a red signal on purpose when he is certain, that the track in front of him is not clear. The possibility of the train driver committing suicide is discussed in the report, but the conclusion is that his emotional imbalance would have caused noticeable changes in his behaviour and driving pattern. His conversation with the train controller had been recorded and both this and the train log have been evaluated by a psychologist.

The southbound train left Rena about 45 seconds before the northbound train left Rustad. I don't think the report mention anything about a relation between the two times.

From this I conclude that the following scenario might have happened [...]

This should not happen. Normal procedure when leaving a station is the following:

\* The train driver notifies the conductor about the green exit signal. The green exit signal is only a sign that the train is allowed to leave the station and is not to be considered as a "leave now" order from the train controller. If the track is free, the exit signal is green already when the train enters the station.

\* The conductor is after he has been notified by the train driver that the exit light is green responsible to be sure that all passengers have left and entered the train and that the departure time has been reached before signalling the train driver to leave.

This makes it reasonable to believe that both the train driver and also the conductor agreed on leaving almost 3 minutes before the time table. The report does not find any reason why that should have happened.

The report ruled out [various concluding] possibilities [suggested by Setzer], with a high degree of probability.

Tor-Einar Jarnbjo

[PGN removed or abridged most of the interstitiated text from Anton.]

---

## **✶ Re: Aasta train crash ... safety-critical error (Setzer, [RISKS-21.28](#))**

Dave Aronson <postmaster@airnsun.dcfido.org>

*Wed, 21 Mar 2001 12:18:11 GMT*

Were it in the USA, I'd also suspect the driver may have been using drugs and alcohol. All in all, though, the only RISK worse than having a human make such decisions is not having a human make such decisions. (With apologies to Oscar Wilde.)

Dave Aronson, Sysop of AirNSun free public Fidonet BBS @ +1-703-

319-0714

---

## **IEEE \*Software\* Special Issue on Building Software Securely**

Anup Ghosh <aghosh@cigital.com>

*Fri, 23 Mar 2001 16:38:00 -0500*

[Here is something that should be of vital interest to RISKS readers and writers alike. PGN]

Call for Articles and Reviewers for an IEEE \*Software Magazine\* Special Issue

"Software Security: Building Systems Securely from the Ground Up"

Publication: January/February 2002, Submission deadline: 1 July 2001

Fragile and insecure software continues to be a major threat to a society increasingly reliant on complex software systems. The premise of this special issue is that most security breaches in practice are made possible by software flaws. We believe engineering secure and robust software systems can break the penetrate-and-patch cycle of software releases all too common today. A constructive exchange on this topic among software practitioners and researchers is the focus of this special issue.

Specifically, our goal is to encourage a deeper, more fully integrated understanding of how security concerns should influence all aspects of software design, implementation, testing, and support. A notorious example

is the buffer overflow problem. Known for decades and very troublesome in networked systems, it continues to be introduced into new software at an alarming rate, due in part to software development habits that trace back to isolated systems where such flaws had few security implications.

An important aspect of this discussion is how to balance security with the many other characteristics of a good software system. Finally, software designers in a networked world cannot pretend to be working in isolation. People are a critical part of the full software security equation, and software that makes unrealistic or unreasonable security-related demands on users (for example, requiring them to memorize too many passwords that change too often) will inevitably fail to keep its data secure. Articles that address the issues of how to design software that works with and directly supports the need for such social engineering issues are also encouraged.

Topics of interest include:

- Case studies that help quantify common security risks
- Security implications of programming languages and development tools
- Techniques for balancing security with other design goals
- Extracting security requirements from software projects
- Design for security
- Developing secure applications
- Aspect-oriented programming for security
- Analyzing programs for vulnerabilities
- Testing for vulnerabilities
- Secure configuration and maintenance
- Developing trusted environments for running untrusted mobile code

- Secure mobile code programming paradigms
- Analyzing unknown software for malicious logic
- Intrusion-tolerant software architectures
- Software application-based intrusion detection
- Models and techniques for quantifying tradeoffs in adding security concerns during development

[... 5,400-word limit, caveats, etc. PGN]

Guest Editors:

Anup K. Ghosh

Director of Security Research, Cigital

phone +1 703 404-9293

anup.ghosh@computer.org <mailto:anup.ghosh@computer.org>

Chuck Howell

Chief Engineer, Joint and Defense-Wide Systems Division, MITRE Corp.

phone +1 703 883-7615

howell@mitre.org <mailto:howell@mitre.org>

James Whittaker

Associate Professor of Computer Science, Florida Institute of Technology

phone +1 321-674-7638

jw@se.fit.edu <mailto:jw@se.fit.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 21: Issue 31**

**Sunday 1 April 2001**

## Contents

- [Windows 2000 source code](#)  
[Mark Thorson](#)
- [Foot-and-mouth virus propagation](#)  
[PGN](#)
- [Upcoming time-change risks](#)  
[Alan Wexelblat](#)
- [More self-inflicted defense difficulties](#)  
[PGN](#)
- [Classification of the Three Mile Island accident](#)  
[Andrew Raybould](#)
- [Re: German armed forces ban MS software](#)  
[Ralf Bendrath](#)
- [What they can do with your SSN](#)  
[Ian Macky](#)
- [Re: Serious new California drivers license ID risk](#)  
[Tom Goltz](#)  
[John Noble](#)
- [Book: Security Engineering, Ross Anderson](#)  
[PGN](#)
- [Invitation to the First "PFIR Future of the Internet Workshop"](#)

[Lauren Weinstein](#)

● [Info on RISKS \(comp.risks\)](#)

---

## ✶ Windows 2000 source code

Mark Thorson <mmm@winery.garlic.com>

Tue, 20 Mar 2001 17:20:38 -0800

Microsoft Corp.'s decision last week to give its 1,000 top U.S. enterprise customers access to the Windows 2000 source code has been sharply criticized by smaller customers. [Source: eWeek (formerly PCWeek), "Windows Source Code Deal: Not For All", March 12, 2001, page 20]

... even more concern was raised by its implementation language, Microsoft Basic. ``Most of our programmers haven't used Basic since college,'' said an IT manager at a Fortune 500 insurance company, ``most OS guys don't consider it [Basic] to be a serious implementation language.''

Mike Conelrad, a senior programmer at an enterprise solution provider based in Kentucky, said he is disappointed that Microsoft has only chosen to release 'desimonymized' source code. ``The original variable names have been replaced with code names like A002134,'' according to Conelrad. ``That tells me absolutely nothing about the variable. But with a name like wParam, at least I know that the variable is word length.''

``Some of the variable names were unacceptable,'' said

Microsoft

spokesperson Lirpa Loof. ``They used trademarks improperly and had other defects which were simply not acceptable in any Microsoft product.''

Sources close to the Windows 2000 development team indicate that the defects include references to Microsoft founder Bill Gates and other officers of the Redmond-based company.

---

## ⚡ **Foot-and-mouth virus propagation**

"Peter G. Neumann" <neumann@csl.sri.com>  
*Sun, 1 Apr 2001 01:02:03 PST*

This bit of satire is very cute. Unfortunately, its copyright keeps us from reproducing it here. Hopefully the given URL will persist. [This item is noted courtesy of Mark Brader.]

Foot-and-mouth believed to be the first virus unable to spread through Microsoft Outlook  
<http://www.satirewire.com/news/0103/outlook.shtml>

---

## ⚡ **Upcoming time-change risks**

Graystreak <wex@media.mit.edu>  
*Wed, 21 Mar 2001 10:45:28 -0500*

[Sorry I could not get this out BEFORE the First of April, as an early warning. But it is still timely. PGN]

I foresee a rash of social engineering set to happen in a few days.

In the USA we change to Daylight Savings Time (spring ahead) shortly after the equinox. By 1966 law, we begin observance on the first Sunday in April, though Congress has a history of mucking about with that date.

This year, that also happens to be the first day in April. In the US (and other countries?) there is a long tradition of practical joking, social engineering, and otherwise just plain messing with people on or around April first.

I can see that this confluence is going to cause some amount of confusion, as some people automatically disbelieve any official-seeming announcement or notice that comes out on or in reference to April 1. Exchanges of the form "Don't forget to set your clocks forward" followed by "yeah, right, funny guy" will likely occur.

Most probably the incidents and losses will be minor and more likely embarrassing than damaging; however, if I was going to try some kind of social engineering feat I'd try to structure it so that it seemed an April Fool's prank if I was caught.

--Alan Wexelblat

P.S. <http://www.standardtime.com/> provides a good explanation of why DST exists and why it's no longer useful.

## ✈ More self-inflicted defense difficulties

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

*Thu, 29 Mar 2001 14:57:22 PST*

On 26 Mar 2001, two U.S. F-15 jets disappeared over Scotland, 45 minutes after takeoff, each with just the pilot on board. One plane was later discovered near the 4,296-foot summit of Scotland's Ben Macdhui, in highest range in Britain.

Also on 26 Mar 2001, a U.S. Army RC-12 reconnaissance plane crashed near Nuremberg, Germany, killing its two pilots.

In all, 58 military people were killed in the 12 months ending on 30 Sep 2000 (including 19 aboard the V-22 Osprey in April 2000, but not the four marines killed on 11 Dec 2000, noted in [RISKS-21.14](#)). Nevertheless, this was reportedly the lowest military accident rate (1.23 per 100,000 flight hours) ever recorded. [Source: AP item, 28 March 2001]

Also, a German military helicopter crashed in Peppen, Germany, on 27 Mar 2001, killing four.

Incidentally, RISKS has not previously noted the most unfortunate recent U.S. submarine exercise that resulted in the sinking of a Japanese fishing vessel. Although the circumstances of that incident are still under investigation, human mistakes seem to have been much more critical than any direct implications of the computer-communication technology.

However, that  
is of course a common thread among many of the life-critical  
incidents  
reported in RISKS.

---

## ✦ Classification of the Three Mile Island accident

"Andrew Raybould" <arayboul@siac.com>

*Mon, 26 Mar 2001 10:52:01 -0500*

This week marks the 22nd anniversary of the Three Mile Island  
accident, and  
while reflecting on that event, it occurred to me that  
describing it as a  
Loss of Coolant Accident (LOCA) doesn't really capture its true  
nature.  
Fundamentally, it was what might be called a Loss of  
Comprehension Accident:  
a minor and correctable problem became the accident it was  
because neither  
the plant's operators, nor the increasingly-senior engineers and  
managers  
brought in as the situation deteriorated beyond recovery,  
understood what  
was happening.

This sort of problem has probably been with us since the  
development of  
organized warfare, but it has increasingly become an issue for  
ordinary life  
as complex control systems have proliferated, starting with  
railroad  
switching and signaling. There is, I understand from this forum  
and  
elsewhere, some concern over whether today's pilots can fully  
understand  
their increasingly-complex airliners (I recall a news item in  
which the

interviewee quoted pilots as saying things like "why did it do that?" "what will it do next?" "how can we make it do..."). As the hardware becomes more reliable, this type of accident becomes relatively more prevalent.

Also, I also strongly suspect that this is a major cause of software development failures: my experience suggests that projects fall apart at that point where the level of detail exceeds the developers' cognitive skills. If so, then the solution will not be found in ever more detailed procedures and standards; we must pay attention to the abstract reasoning and language skills that are necessary for a group of developers to understand, individually and collectively, what it is that they are doing.

Andrew Raybould    andy.raybould@att.net

---

## **✶ Re: German armed forces ban MS software (McVay, [RISKS-21.30](#))**

Ralf Bendrath <bendrath@zedat.fu-berlin.de>

*Sat, 24 Mar 2001 03:16:12 -0600*

This news is old and wrong - the German armed forces immediately told the press that they still use Microsoft products. Actually they just bought a general licence for MS standard office applications half a year ago. They even use Lotus Notes, which is known for the "work factor reduction field"

in its encryption keys - and these are known to the NSA. But the Bundeswehr is not that stupid - they just put everything through hardware encryption (as far as I remember from Siemens) additionally. I only have a German article on this update, sorry.

Ralf Bendrath Listowner Infowar.de <http://userpage.fu-berlin.de/~bendrath>

Update: Bundeswehr setzt weiter auf MS-Software (tecChannel.de, 19 Mar 2001)

Das Verteidigungsministerium hat gegenueber tecChannel.de einen Bericht des Nachrichtenmagazins Der Spiegel dementiert, wonach die Bundeswehr kuenftig in Computern keine Software von Microsoft mehr einsetzen werde. Wie berichtet, heisst es in dem Artikel "Die Angst der Deutschen vor amerikanischer Spionage", der amerikanische Geheimdienst NSA habe nach Erkenntnissen deutscher Sicherheitsbehoerden Zugriff auf alle wichtigen Quellcodes von Microsoft Dadurch koenne er auch verschluesselte Daten lesen. Das Verteidigungsministerium wolle daher in sensiblen Bereichen kuenftig nur noch Verschluesselungstechniken der deutschen Firmen Siemens und der Telekom einsetzen, um seine Geheimnisse zu schuetzen, so der Spiegel. Ein Sprecher des Bundesministeriums fuer Verteidigung hat den Spiegel-Bericht jetzt gegenueber tecChannel.de dementiert. In einem Fax, das die Redaktion vor wenigen Minuten erreichte, heisst es: "Die Behauptung, die Bundeswehr werde in sensiblen Bereichen kuenftig keine Software der Firma Microsoft mehr verwenden, ist falsch." Die Bundeswehr habe demnach erst vor einem halben Jahr einen Generallizenzvertrag ueber die

handelsueblichen  
Softwareprodukte mit Microsoft abgeschlossen. "Die Bundeswehr  
beabsichtigt,  
diese Produkte auch weiterhin einzusetzen", so der Sprecher  
weiter. Er  
betonte, dass sensible Daten im IT-Bereich der Bundeswehr zum  
einen durch  
Firewalls gesichert seien. Zum anderen setze die Bundeswehr auf  
Verschlüsselungstechniken, "die durch das Bundesamt fuer  
Sicherheit in der  
Informationstechnologie (BSI) zugelassen sind. Deren  
Schutzfunktionen  
arbeiten unabhängig von der benutzten Software", heisst es in der  
Mitteilung. (jma)

---

## ⚡ What they can do with your SSN

Ian Macky <imacky@us.oracle.com>  
*Sat, 24 Mar 2001 14:07:52 -0800 (PST)*

In March of this year, 2001, in which it is proven that we are  
all very  
smart monkeys indeed, I received my monthly mortgage statement  
and noticed  
in the bottom IMPORTANT MESSAGES section:

YOUR MORTGAGE INFORMATION IS NOW AVAILABLE ONLINE! [Note,  
feel  
dreadful sort of arousal here, like anticipation of being  
screwed]  
JUST FOLLOW THESE STEPS: 1. GO TO WWW.xyz.COM [Censored] 2.  
CLICK  
ON "MY HOME LOAN ACCOUNT" 3. ENTER YOUR ACCOUNT NUMBER 4.  
ENTER  
YOUR PASSWORD (YOUR STATE ABBREVIATION & THE LAST 4 DIGITS  
OF THE  
PRIMARY BORROWER'S SOCIAL SECURITY NUMBER, EXAMPLE NY1234).

On this same piece of paper are my account number and state

abbreviation.

Yet ``it's unlikely and unusual for someone who has your Social Security number to be able to do anything with it. Normally, financial institutions require additional information.''

"Unlikely", "unusual". Pretty squirmy. And that additional information sure was hard to come by.

BTW, my mortgage holder is a colossus whom everyone has heard of. Large body does not equal large brain when it comes to corporations--the area of the pyramid's tip remains constant (and small!).

---

## ⚡ **Re: Serious new California drivers license ID risk (Cornell, [R-21.29](#))**

Tom Goltz <tgoltz@QuietSoftware.com>  
*Sun, 25 Mar 2001 20:48:30 -0500*

[From Dave Farber's IP distribution]

Ironically, the fake doesn't even have to be very good. A couple of facts that you may find interesting:

I am white. I have held a California driver's license in the past, but that license has been inactive for over two years since I established residency in another state.

In October of last year, a black male obtained a fake California driver's license with my name on it and his picture. The driver's

license ID # he used belongs to a white female. The address is a Commercial Mail Receiving Agency in Costa Mesa CA, which the state doesn't normally allow. The fake also contained two spelling errors.

This person used this ID and my social security number to open a dozen different credit accounts in my name at various locations around the Los Angeles area. He was using a cell phone with a phone number based in the 603 area code as his residence phone.

If anyone had bothered to look, just about everything about this guy screamed fraud, yet he managed to steal \$15,000 worth of merchandise (mostly jewelry).

Out of all these people who were supposed to be checking this information, only TWO found problems. One was a used car dealer who became suspicious when the check this guy gave for the down payment proved to be bogus. They refused to give the guy the car, but didn't bother to pursue the matter with the police. The other was store security at a Costco in Las Vegas, who tracked me down in New Hampshire and informed me that I had a problem. They detained the man, and turned him over to the police.

Sadly, the most he's going to do is a couple of years probation - he didn't actually steal anything in Las Vegas, and the identity theft, although a crime in NV is not sufficient to assure jail time by itself. I discussed the matter of extraditing the varmint to California with Las Vegas police, but they told me that it was unlikely that California would

bother for something that would only net the offender probation there as well. According to the LV police detective, in California, you have to be charged with stealing over \$50,000 before you'll do any jail time.

It's no wonder this crime is exploding...it's low risk, extremely profitable, and trivial to implement.

Oh yes...how did he get my name and social security number? He told the Las Vegas police that he purchased the information on the street for \$500.

Tom Goltz, Software Engineering Services (603) 594-9922

---

## **⚡ Re: Serious new California drivers license ID risk (Cornell, [R-21.29](#))**

John Noble <jnoble@dgsys.com>  
*Mon, 26 Mar 2001 06:17:46 -0500*

[From Dave Farber's IP distribution]

I'm a recovering bank lawyer who hasn't had a serious lapse in nearly ten years, but I find I can't help myself. The account of the fraud perpetrated with a forged drivers license and the supposed complicity of Wells Fargo and California law is misinformed and misinforms your subscribers. It has nothing to do with the real risks identified in the Risk Digest item he points to.

Although drivers licenses are increasingly designed to be more

difficult to duplicate than they used to be, you can forge anything with the right equipment. There is nothing new about that. People have been forging identification and cashing bad checks since they invented banks. Whatever the problem with the CA license, it is not obvious how it contributes to the fraud Mr. Cornell describes. The fact that the lic. no. and DOB is recorded on a magnetic strip instead of printed on the license only makes it that much harder to discover, and that much harder to duplicate. Mr. Cornell indicates that he wants one without a photo. How does that help? Cornell's photo-free driver's license is only going to prevent him from cashing checks. It isn't going to stop someone else with a forged license that does have a picture unless he can find a bank that requires DNA testing to cash a check.

Mr. Cornell's description of the CA Commercial Code leaves out the good parts. An account may be debited if the item was "properly paid," i.e. "authorized" in fact. If the item was not authorized, the customer need only notify the bank within a reasonable time after receiving his statement to have the account re-credited -- the burden is on the bank to prove that the endorsement was genuine, which is impossible. Banks typically ask the customer to sign an affidavit; and they pull the video sequence of the transaction at the teller window to confirm that the customer did not cash the check himself (the unlikely exception to the impossibility of proving

the endorsement was genuine). Mr. Cornell points to Code provisions that require the victim to "prove" that the bank failed to exercise "ordinary care." But the provision only applies to losses caused by the customer's failure to review his bank statement and report an unauthorized debit within a reasonable time. In effect the bank is strictly liable for unauthorized debits during the first 6-8 weeks on little more than the customer's insistence that they were unauthorized. But if the customer doesn't look at his statement and report the unauthorized transactions disclosed on the statement, the bank's liability is cut off and the customer is stuck with the additional losses. The reasons for this are obvious. Only the customer is in a position to know that the debit was unauthorized. If he doesn't look at his statements, and the same guy is cleaning him out month after month, whose fault is that? In addition, the law has to take into account the possibility that the customer is having his own checks cashed by a third party.

If Cornell has scoured the internet without finding it mentioned, it is because it is relatively rare. This is a risky, complicated, inefficient and finally stupid way to steal money. Someone has to make the ID (holograms, magnetic strips encoded with the drivers lic. no. and DOB); then stand at the teller's window in front of a camera posing for the wanted poster. Moreover, when you cash a check that bounces, the bank doesn't wait until the end of the statement cycle to let you know about it. They send you

a letter. You would need to ignore those letters, as well as your bank statement, to lose the tens of thousands of dollars Cornell reports. When the forger cashes a check for which the the bank isn't liable, 6-8 weeks after he cashed the first check, the forger needs to assume that the victim has ignored the letters and statement -- because otherwise he's busted. Anybody who has your bank account no. can far more easily create checks that carry your name and account number. He doesn't need your drivers lic. no., DOB, or soc. sec. no. for that. He just draws against your account on checks coded with your account no.; deposits them in a straw account; withdraws the funds and closes the account before your statement goes out; and moves on to another bank and another victim because he has to assume you reported the fraud. He can do all that without ever having his picture taken for either a fake drivers license or a wanted poster. He doesn't have to stand at the teller window in your bank wondering whether he's about to get busted because you reviewed your statement and reported the fraud, and his picture from the videotape has been circulated to the tellers and security personnel. He can move the money and close the account from the safety of his apartment using his computer. The moral of the story: review your bank statements -- it's part of the deal. John Noble

---

**🔥 Book: Security Engineering, Ross Anderson**

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

*Thu, 29 Mar 2001 16:12:17 PST*

Ross Anderson

Security Engineering: A Guide to Building Dependable Distributed Systems

John Wiley & Sons

March 2001

xxviii+612 pp.

ISBN 0-471-38922-6

This book is an enormous undertaking. The chapter titles suggest the breadth of coverage.

Part 1 (basic concepts)

1. What is security engineering
2. Protocols
3. Passwords
4. Access controls
5. Cryptography
6. Distributed systems

Part 2 (important applications)

7. Multilevel security
8. Multilateral security
9. Banking and bookkeeping
10. Monitoring systems
11. Nuclear command and control
12. Security printing and seals
13. Biometrics
14. Physical tamper resistance
15. Emission security
16. Electronic and information warfare
17. Telcom system security
18. Network attack and defense
19. Protecting e-commerce systems
20. Copyright and privacy protection

Part 3 (organizational and policy issues)

21. E-policy
22. Management issues
23. System evaluation and assurance

## 24. Conclusions

Although there are other books that delve into greater detail on specific topics, this book should be extremely useful to many people who need the overall system perspective that Ross provides.

Ross's preface concludes with this sentence:

"I believe that building systems that continue to perform robustly in the face of malice is one of the most important, interesting, and difficult tasks facing engineers in the twenty-first century."

I could not agree more, although I would add that building systems to perform robustly in the face of arbitrary adversities (accommodating power and communication losses, rodents, bad software engineering, user errors, etc. -- that is, not merely accounting for malice) is even more challenging. Many systems in common use tend to fall apart all by themselves -- without any malice!

---

## **Invitation to the First "PFIR Future of the Internet Workshop"**

Lauren Weinstein <lauren@pfir.org>  
*Sat, 31 Mar 2001 16:13:40 -0800 (PST)*

"PFIR Future of the Internet Workshop"

From: Lauren Weinstein  
lauren@pfir.org  
lauren@vortex.com

Peter G. Neumann  
neumann@pfir.org  
neumann@csl.sri.com

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

Greetings. People For Internet Responsibility (PFIR), in conjunction with the ACM Committee on Computers and Public Policy, is pleased to announce the first "PFIR Future of the Internet Workshop," to be held on the weekend of May 5 and 6, 2001, at the Culver City Veterans Memorial Complex, just minutes from Los Angeles International (LAX) airport. Vortex Technology of Woodland Hills, California is handling the event logistics.

Information about PFIR, and the current PFIR position papers, are available at: <http://www.pfir.org>.

This very small event will bring together for open discussions some of the Internet's most important "doers" (including Dave Farber, former Chief Scientist for the FCC and a founding member of the PFIR Board of Directors). The workshop is aimed at encouraging discourse with and among the persons who have not only been responsible for helping to get the Internet (and its ancestor ARPANET) to the level we know today, but are also leading in doing the actual work of helping to guide the Net's future.

The workshop (which we want to limit to around 40 attendees) will be interdisciplinary in focus. It will also be informal, low-key, basically utilitarian, and largely off-the-record. There will be no formal paper presentations, no exhibits, and while we expect attendance by one or two major technology reporters, they will be coming mainly as

individual

participants and will have agreed not to report on the content of off-the-record discussions.

Because space will be limited, and we wish to encourage a diversity of attendees (in terms of interests, specialties, and geography), we cannot guarantee that everyone who wishes to attend will be able to do so. In such a circumstance, we'll choose among prospective attendees in a manner that will hopefully enhance the usefulness of the workshop for everyone concerned.

Unless otherwise prearranged in particular cases, all attendees must be registered in advance of the event.

A framework agenda of the conference will be discussed via e-mail among participants during the weeks before the event, but it is expected that a variety of the topics listed in the PFIR Issues document (<http://www.pfir.org/issues>) will be of interest. The agenda will be subject to change at the workshop as participants see fit. The Internet is of course an international medium, and international issues should be of significant importance in the discussions. Any topics of relevance to the Internet, from domain names to governmental controls, from censorship to intellectual property protections, from infrastructure to law enforcement, and any others of interest, will be fair game during our discussions.

As Internet-related issues have come to pervade ever more aspects of our society, reasoned discourse regarding many of these issues has increasingly

been drowned out by a sea of emotional e-mail interactions and hardening uncooperative positions. This workshop will present an opportunity to meet face-to-face for two days of intelligent conversations as human beings, as we try to chart some possible solutions and courses for the range of difficult challenges the Internet (and society's reactions to the Net) have presented to us.

We're trying to keep the workshop as simple as possible. We'll be charging a small registration fee (about \$85) to help defray costs. This amount will include continental breakfast and a lunch both days. There are a number of reasonably-priced hotels in the area. L.A. being what it is, you'd probably want to rent a car, though some car-pooling arrangements can possibly be worked out if there is interest. The workshop will run from 9 AM to 4:30 PM on Saturday May 5, and from 9 AM to 3:00 PM on Sunday May 6. We'd like to handle most or all of the registrations before the actual event if possible. Details on this and other related information (hotel lists, etc.) will be provided later.

If you're interested in attending, or if you have other questions about the workshop purpose, agenda, or other associated matters, please send an e-mail note to:

[workshop@pfir.org](mailto:workshop@pfir.org)

Please be sure to mention your areas of interest and specialties relating to Internet issues.

We'd also be happy to chat by phone at the numbers listed below. Questions regarding ongoing workshop operational issues (registrations, information about the area or other assistance and questions, etc.) should be directed to Susie Hirsch (susie@pfir.org). You can contact Susie by phone at: (310) 737-1739.

We hope that you'll consider attending! Please let us know if you're interested, at your earliest opportunity, and we'll keep you on the information list. Because this is a small event, every attendee is especially important, and we're doing our utmost to bring together a fascinating and somewhat eclectic group of "movers and shakers" who, working together, can help the Internet better serve everyone, everywhere.

We look forward to hearing from you. Thank you very much.

Lauren Weinstein  
lauren@pfir.org or lauren@vortex.com  
(818) 225-2800  
Co-Founder, PFIR - People For Internet Responsibility - <http://www.pfir.org>  
Moderator, PRIVACY Forum - <http://www.vortex.com>  
Member, ACM Committee on Computers and Public Policy

Peter G. Neumann  
neumann@pfir.org or neumann@csl.sri.com  
(650) 859-2375  
Co-Founder, PFIR - People For Internet Responsibility - <http://www.pfir.org>  
Moderator, RISKS Forum - <http://catless.ncl.ac.uk/Risks>  
Chairman, ACM Committee on Computers and Public Policy



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 21: Issue 32**

**Monday 2 April 2001**

## Contents

- [Future Mac Viruses?](#)  
[PC Rescue](#)
- [The cost of Windows virus](#)  
[Joaquim Baptista](#)
- [Risks of auto-updating software](#)  
[Alan Wexelblat](#)
- [Dutch police fight cell theft with text 'bombs'](#)  
[Thomas Dzubin](#)
- [Cellphone text bombs](#)  
[Conrad Heiney](#)
- [Approved posts to large listservs](#)  
[Paul Hessels](#)
- [MSN "upgrade" creates long-distance calling](#)  
[Steve Holzworth](#)
- [Re: Hidden info on MS Word documents](#)  
[Joaquim Baptista](#)
- [Hidden highway robbery within Terms of Use contracts?](#)  
[Michael Sinz](#)
- [EoExchange shuts down services without warning, customer data lost](#)  
[Derek Ziglar](#)

- [Re: "Internet Voting is no 'Magic Ballot'"](#)  
[Jay R. Ashworth](#)  
[Jurek Kirakowski](#)
  - [Re: Bogus Microsoft Corporation digital certificates](#)  
[Peter da Silva](#)  
[WBH](#)
  - [Re: Verisign certificates problem](#)  
[Camillo Sars](#)
  - [Re: Aasta train crash](#)  
[Dag-Erling Smorgrav](#)
  - [Re: Serious new CA Drivers License ID RISK](#)  
[Jim Horning](#)  
[John Rickenbrode](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

## ⚡ Future Mac Viruses?

"PC Rescue" <paul@pcrescue.com.au>  
*Sun, 25 Mar 2001 06:48:30 +1000*

Mac users have been crowing for some time that their system is less prone to viruses than the horrible alternative. Could this be about to change?

<http://www.wirednews.com/news/technology/0,1282,42586,00.html>

"The box contains three installation CDs -- Mac OS X, Mac OS 9.1 and a CD full of developer tools, including the Cocoa programming environment, which is reportedly simple enough for school kids to use."

www.pcrescue.com.au info@pcrescue.com.au Tel 0415 967 017  
Fax: 02 9953 8772

## **✶ The cost of Windows virus**

Joaquim Baptista <px@altitude.com>

*Tue, 27 Mar 2001 22:44:32 +0000*

I am deploying a custom-made server program that makes several manipulations of XML files, including an automated conversion to Word.

It had been a mystery why the production server, a Pentium 700 with SCSI disks running Windows 2000, was much slower than the development server, a Pentium 500 with IDE disks.

Yesterday, a particular long processing involving a 53MB RTF file just run forever. I killed it consumed after 3 hours of CPU.

Then, we decided to turn off the anti-virus software. A sample task that took over six minutes now takes two and a half minutes. And the very long processing now runs in 15 minutes.

Therefore, the cost of the Windows virus includes the cost of running the anti-virus software. It cripples my server to less than half its performance. My Pentium 700 becomes a Pentium 270 (usual case)! On some cases, the anti-virus software delays the computation at least 24 times, and the Pentium 700 becomes less than a Pentium 30!

Linux suddenly seems a lot cheaper!

Joaquim Baptista, alias pxQuim, Director, Technical Documentation  
px@altitude.com

## ⚡ Risks of auto-updating software

Graystreak <wex@media.mit.edu>

*Sun, 1 Apr 2001 11:49:52 -0400*

In his recent (April 2001) AskTog column, Bruce Toganzzini reports on his ReplayTV which, one recent day, updated itself to disable a valuable feature.

<http://www.asktog.com/columns/045ReplayTV.html>

We saw something like this happen when Napster first tried to ban Metallica song-trading -- they forced users to update to a new client which had the blocking patch installed. This is the first mass-market product (as in, people paid lots of real money for this) instance of this that I can think of.

I'm certain it won't be the last. We are moving to a realm of always-on, always-connected devices. In this realm, our software will begin misbehaving without our ever doing anything to it.

Alan Wexelblat, moderator, rec.arts.sf.reviews wex@media.mit.edu  
<http://wex.www.media.mit.edu/people/wex/>

---

## ⚡ Dutch police fight cell theft with text 'bombs'

Thomas Dzubin <dzubint@vcn.bc.ca>

*Wed, 28 Mar 2001 11:49:11 -0800 (PST)*

After a user reports his GSM handset stolen, the police start sending out one Short Message Service text message to the phone every three minutes: "This handset was nicked, buying or selling is a crime. The police."

See web page story at:

<http://www.cnn.com/2001/TECH/ptech/03/28/SMS.bomb.idg/index.html>

Thomas Dzubin, Vancouver, Saskatoon, or Calgary CANADA

---

## 🔥 Cellphone text bombs

"Conrad Heiney" <conrad@fringehead.org>

*Wed, 28 Mar 2001 09:21:51 -0800*

CNN and IDG report

<http://www.cnn.com/2001/TECH/ptech/03/28/SMS.bomb.idg/index.html>

that the Dutch police are using a kind of mailbomb technique to discourage theft of wireless phones.

If a phone is believed to be stolen, police track it down with its unique identification number and send the message "This handset was nicked, buying or selling it is a crime" every three minutes via SMS.

The RISK here is fairly obvious. What to do if your phone ends up mysteriously on the 'stolen' list? Go to your local police station? The phone company?

Conrad Heiney   conrad@fringehead.org   <http://fringehead.org/>

## ✶ Approved posts to large listservs

Paul Hessels <timdau@yahoo.com>

*Thu, 29 Mar 2001 12:21:17 -0800 (PST)*

I recently sent an email to bugtraq@securityfocus.com, which was approved after being examined by the moderator.

Here is the risk: Since I made the mistake of using an e-mail address from a small domain that I manage, my DNS server immediately got killed by the tens of thousands of mail servers trying to resolve my domain name. (which of course was not in anyones cache; my domain is pretty much unknown.)

I saw all this traffic and didn't immediately recognize what it was. I was scared, but a little bit of investigation provided an answer.

After an hour and my cable modem rebooting a few times from the sheer load, everything seemed to settle down, but I'll tell you, watching the lights on that modem flash without yet understanding what was happening sure scared me.

---

## ✶ MSN "upgrade" creates long-distance calling

Steve Holzworth <sch@unx.sas.com>

*Fri, 30 Mar 2001 18:24:20 -0500*

As RISKS readers are aware, automatic upgrades of software aren't always as innocuous as "they" would have you believe. A recent Microsoft Networks (MSN) dial-up upgrade caused some users in the Research Triangle, NC area to suddenly start dialing in via a long distance access number, as opposed to the previously local exchange. WRAL TV's consumer reporter has received 51 calls about this so far.

Someone's phone bill included \$361 in long distance charges to a Chapel Hill number for his Internet connection through Microsoft Networks, despite having used a local number. An MSN customer service representative told someone else that MSN "lost local numbers for several areas" during an upgrade. Several complainants had online chats where representatives insisted the Chapel Hill number was not long distance." [Source: WRAL TV online (excerpted [and PGN-ed])

<http://www.wral-tv.com/features/5onyourside/2001/0329-msn-folo/>]

Adding additional dial-in numbers may be a good thing for a service to do. Arbitrarily changing the numbers that existing customers chose to use, without at least warning the customers first, seems rather suspect, as MSN has now discovered. Compounding the error by telling your customers that they are mistaken, while said customers are holding their long distance bills in their hands, certainly inspires confidence...

Steve Holzworth, Senior Systems Developer, SAS Institute - Open Systems R&D VMS/MAC/UNIX, Cary, N.C. sch@unx.sas.com

## **⚡ Re: Hidden info on MS Word documents (Henry, [RISKS-21.25](#))**

Joaquim Baptista <px@altitude.com>

*Tue, 27 Mar 2001 21:56:04 +0000*

>Mitigation: Use RTF when you can -- no hidden info, no viruses.

...unless your document includes images. Images store their pathname, even in RTF, although the ASCII characters are "hidden" as hexadecimal numbers.

I have actually used this "feature" to recover the original images included in Word documents.

Joaquim Baptista, alias pxQuim, Director, Technical Documentation  
px@altitude.com

---

## **⚡ Hidden highway robbery within Terms of Use contracts?**

Michael Sinz <Michael.Sinz@sinz.org>

*Fri, 30 Mar 2001 17:46:04 -0500*

Can this ever be considered not unreasonable?

If you use .NET and/or HailStorm PassPort service, you will find that basically you are giving everything to Microsoft.

If you send source code or business plans or a chapter of your first novel or anything else of any value (or of no value), Microsoft has the right to use, exploit, and sublicense any and or all of it without any

payment to the  
copyright holder. It also has the right to any trademark,  
service mark, or  
patent that you might use in such communications or documents  
that are  
used/stored/transmitted via their service!

See <http://www.passport.com/Consumer/TermsOfUse.asp>

So, when Windows and Office get .NET'ed, don't expect to be able  
to use  
Windows or Office for anything that you want to keep for  
yourself.

Microsoft says "All your data belong to us"

And it really is not a joke, given their own legal terms of use  
documents.

I guess program development for the Windows platform now will  
need to be  
done on some non-.NET systems - otherwise you may as well just  
give your  
software to Microsoft. (And your business plans, and poetry,  
and payroll  
data, and...)

Look at the section "License to Microsoft"

Quote:

LICENSE TO MICROSOFT

By posting messages, uploading files, inputting data,  
submitting any  
feedback or suggestions, or engaging in any other form of  
communication  
with or through the Passport Web Site, you warrant and  
represent that you  
own or otherwise control the rights necessary to do so and you  
are  
granting Microsoft and its affiliated companies permission to:

1. Use, modify, copy, distribute, transmit, publicly display,

publicly

perform, reproduce, publish, sublicense, create derivative works from, transfer, or sell any such communication.

2. Sublicense to third parties the unrestricted right to exercise any of the foregoing rights granted with respect to the communication.

3. Publish your name in connection with any such communication.

The foregoing grants shall include the right to exploit any proprietary

rights in such communication, including but not limited to rights under

copyright, trademark, service mark or patent laws under any relevant

jurisdiction. No compensation will be paid with respect to Microsoft's

use of the materials contained within such communication. Microsoft is

under no obligation to post or use any materials you may provide and may

remove such materials at any time in Microsoft's sole discretion.

:End-Quote

Talk about trying to own the world. Using the ".NET" Word to write

up your patent would give Microsoft rights to use the patent. Sending

information about your patent via MSN EMail or IM does the same.

Can such a Terms of Use even be enforced?

Just when you thought the worst of Microsoft, you find something that proves that you have not gotten there yet.

Michael Sinz ---- Technology and Engineering Director/Consultant  
michael.sinz@sinz.org <http://www.sinz.org/Michael.Sinz>

## ⚡ EoExchange shuts down services without warning, customer data lost

"Derek Ziglar" <dziglar@yahoo.com>

Tue, 27 Mar 2001 08:39:54 -0500

We've long known the risk of course is depending on 'free' and advertiser supported services--since they are free to the user, the provider is under no obligation to continue them.

Last week, EoExchange shut down their multiple advertiser-supported services they have been offering on the web for several years. These included EoMonitor (web page change monitoring better than anything else I had ever seen), EgoSurf (a name-oriented search engine) and Daily Diffis (tracked content changes across many informative sites).

The real Risk here to the users was that EoExchange chose to discontinue them \*without\* advance notice. On Tuesday, the services were operating normally. On Thursday, the sites were inaccessible and merely forwarded to a corporate web page promoting different products.

Suddenly and without warning, users of these services could no longer access the user-specific stored data they had accumulated through them. These included lists of favorite links and web sites, many of which people depended on regularly for information. The complete lack of warning meant none of the users had the opportunity to print off their

personal data from  
the sites and preserve these lists of important sites.

Adding insult to injury is the company's complete lack of an explanation, even after the fact. All users of these services simply find the URLs now redirecting to a corporate site that neither apologizes for the shutdown nor even acknowledges that these services ever existed. When I contacted the company for an explanation, I received only a vague reply that they had chosen to discontinue the advertiser-supported services and focus on their corporate solutions.

So this was a not-very-subtitle reminder that when using any 'free' online services where you store personal and needed data (emails, lists of links, etc.), don't forget to make some kind of regular backup--even if only simple printouts--of your data there in case the services shut down unexpectedly.

Derek Ziglar, Atlanta, Georgia dziglar@yahoo.com

---

**⚡ Re: "Internet Voting is no 'Magic Ballot'" (Jones, [RISKS-21.30](#))**

"Jay R. Ashworth" <jra@baylink.com>  
*Tue, 27 Mar 2001 10:18:15 -0500*

In his comments to RISKS, Douglas Jones asserts that electronic, and more specifically \*Internet\*, voting is just like absentee balloting, and that therefore, it doesn't really merit any more special lawmaking or

concern --

we just need to enforce the laws we already have concerning such ballots.

I disagree.

All voting systems are tradeoffs, as nearly everyone interested in the topic has been reminded repeatedly since 7 November 2000. Different tradeoffs have traditionally been made for absentee ballots, since elections as close as the 2000 Presidential election are quite uncommon, and therefore relaxing the constraints on absentee votes is an acceptable tradeoff for \*getting\* those votes -- that is, making it possible for people who could not otherwise vote to be heard.

But, these relaxed strictures are only acceptable, so far as I can see, precisely \*because\* those votes are such a small percentage of the total (well under 1%, usually). It would \*not\* be acceptable to use restrictions that loose for a voting method that might collect 30-50%, or even more, of the total balloting.

The most notable criterion in question is secrecy of vote. This is in place, as <http://www.research.att.com/~lorrie/voting/>; >Lorrie Cranor's excellent e-voting compendium</a> would remind us, to prevent vote-selling. "Oh, but no one does that these days -- well, except maybe in Chicago" (:-).

Nope. The restriction \*works\*. And, honestly, I cannot see \*any way at all\* to \*impose\* that restriction on voting which may be done

from home.

You can't even be *\*certain\** that a vote came from whom it says it did; Bruce

Schneier has explained fairly clearly in his Crypto-Gram newsletters the pitfalls in depending on even digital signatures, for something this important.

While the various people involved, according to general press accounts, seem to properly appreciate the stringent requirements of electronic voting in precincts -- chief among them the point that a "vote" needs

to be a (rugged) *\*physical object that the voter can inspect, completed\** (I'm thinking of OCR printing on Polaroid film, myself) --

I don't think the problem of Internet voting at home is soluble.

Though I'm willing to be convinced otherwise. It won't be easy.

Jay R. Ashworth, Member of the Technical Staff, Baylink, The Suncoast Freenet  
Tampa Bay, Florida <http://baylink.pitas.com> +1 727 804 5015  
jra@baylink.com

---

**⚡ Re: "Internet Voting is no 'Magic Ballot'" (Jones, [RISKS-21.30](#))**

jk <jzk@ucc.ie>

*Tue, 27 Mar 2001 12:16:33 +0100*

Douglas W. Jones raised the problems of user-testing the DRE machines, citing among other reasons, that "A voter casts only one ballot, and for the voter, the voting experience is a peak moment" one may add also that

voting is not a frequent activity so there will also usually be an element of uncertainty when confronted with the interface to be used... especially if the interface has changed (maybe for the better) since last time.

In usability testing, an important issue is the 'Context of Use' (see <http://www.ucc.ie/hfrg/baseline/filearchive.html#cou> ) which boils down to the idea that a 'usability test' can be extremely misleading if carried out under conditions which do not mirror the real-life conditions in important respects. And emotionality, stress, and uncertainty are crucial features of this situation which will affect the results of any test.

The basic tenet is: context of test = context of use.

The best check on this kind of software would be to have the keypad or screen physically wired up to a completely separate second local system which will record the tallies using an algorithm independent of the main system, and to test it in situations as close to the real as possible. Telling pretend users to go in and punch a set of buttons is, I agree, not a very realistic way of testing; using over-the-shoulder video technology is incredibly time-consuming and will bring in its own sources of rater error.

Jurek Kirakowski, HFRG, Ireland <http://hfrg.ucc.ie/> <http://hfrg.ucc.ie/jk/>

**⚡ Re: Bogus Microsoft Corporation digital certificates (Savit, [R-21.30](#))**

Peter da Silva <peter@abnm.com>  
*Mon, 26 Mar 2001 12:10:10 -0600 (CST)*

The real risk here is the protection model used by Internet Explorer and related programs. Rather than establishing a mechanism whereby active content can be run (possibly with somewhat degraded performance) in a sandbox, it depends on all the certificant's being able to ensure that their certificates and signed applets are secure.

Certificates are useful as an additional mechanism on top of a secure system, to provide accountability, but they're no replacement for one.

---

**⚡ Re: Bogus Microsoft Corporation digital certificates (Savit, [R-21.30](#))**

WBH <mustang@erols.com>  
*Fri, 23 Mar 2001 21:42:37 -0500*

Microsoft isn't the primary victim, WE ARE!!

The only way to practically resolve this issue is for Verisign to re-issue all certs they ever verified under a new CA signing certificate. THEN, Verisign has to launch a campaign to replace it's CA certs in every online users' web browser!!

Why? Because the general public (us) doesn't have a CRL-checking mechanism when our browsers verify a certificate as valid. Our browsers only look as far as the list of CA certificates that are embedded in our browser at the time we verify a cert.

This isn't a minor PKI flap.

THIS IS HUGE SECURITY DEBACLE FOR VERISIGN, AND A MAJOR NEW VULNERABILITY FOR THE ONLINE PUBLIC AT LARGE!!!

---

## ✶ Re: Verisign certificates problem (Sinclair, [RISKS-21.30](#))

"Camillo Sars" <ged@iki.fi>  
27 Mar 2001 12:47:37 +0300

> [...] do not have this CRL Distribution Point field properly filled in.

Unfortunately, the problem lies much deeper. The CDP field is not mandatory, it is *optional*. Complying implementations are supposed to "know" where to get the CRL in case the CDP field is not filled in. In most cases, configuring the CDP for the CA in these cases should be done at the same time as the CA certificate is given "trusted" status. That is, in theory at least.

There is no real standard for how "certificates" should be filled in, issued or used. The often cited X.509 standard is very loose, and requires

significant profiling to suit a particular purpose. The profiling work for Internet use has only recently produced the first IETF RFC:s. For those who are familiar with the risks caused by directory lookups based on "common names", it is interesting to note that one of the tricky parts of the IETF work was to come to an agreement as to what is part of a "unique name". I'm not sure a compromise is good risk management in this case...

Current "X.509 certificates" are suitable for deployment in specialized environments, but anyone relying on them for what one might call "generic Internet authentication" needs to be aware of the pitfalls. The risk? Only a handful of people worldwide really know enough to be able to estimate the risks, but still we rely on things like SSL daily. Ask yourself - Do You know how your favorite browser responds to different PKI violations? And how would You respond?

For a good, albeit rather specialized, view on PKIs, I recommend reading Bruce Schneier's book "Secrets and Lies". Bruce also co-authored a paper on "Ten risks of PKI" with Carl Ellison, which is probably a "must-read" for regular RISKS readers.

> Two things need to be done, one is that software which checks certificates  
> must be changed to warn users that certificates lacking a CRL are much more  
> suspect and Verisign needs to re-place all certificates that currently lack  
> this critical information with new certificates that have this field  
> properly filled in.

Also note the risk caused by implementing strict CRL checks. The CDP becomes a single point-of-failure for any relying certificates. I have experienced a situation where a software update at the CA site caused relying clients to fail in their CRL requests. If a site relies heavily on certificate-based authentication, the consequences can be very severe.

Camillo Särs <+ged@iki.fi> <<http://www.iki.fi/+ged>>

---

## ✶ Re: Aasta train crash (Jarnbjo, [RISKS-21.30](#))

Dag-Erling Smorgrav <des@thinksec.com>  
27 Mar 2001 12:26:38 +0200

> [...] As this service had been canceled by the operator Telenor, all  
> train drivers had to call the train controlling central and report their  
> train number and the corresponding mobile phone number.

This is incorrect. Telenor did not cancel NSB's phone service; the report clearly states that NSB had changed their train numbering scheme so that train numbers were no longer within the number range allocated to them by Telenor.

I find it distasteful that people are still trying to invent reasons to absolve NSB of the responsibility for this and the numerous other accidents and interruptions of service they had last year. NSB's shoddy

management,  
total lack of respect for their customers (though I have to admit they're still more customer-oriented than Oslo's public transportation authority, who seem to regard every passenger as a potentially violent criminal), and mismanagement of funds - spending billions on prestige projects with practically no ROI, while letting their infrastructure and equipment deteriorate for lack of maintenance - are the deep causes of these accidents.

Dag-Erling Smørgrav - des@thinksec.com

---

## ✦ **Re: Serious new CA Drivers License ID RISK (Cornell, [RISKS-21.29](#))**

Jim Horning <horning@intertrust.com>

*Wed, 28 Mar 2001 10:51:00 -0800*

Back in August 1997, in [RISKS 19.28](#), I reported the identical scam being pulled on me, involving the same bank (Wells Fargo). At that time, my local branch manager told me that she was currently working with three other customers of THAT BRANCH to put their banking accounts back in order as a result of the same scam.

That was before Wells Fargo was bought by an out-of-state bank (that changed its name to Wells Fargo), and I must say that all the bank employees, both in the branch and in the fraud detection department, were

cooperative and helpful, and in the end I was only out time, not cash. But it was still a damn nuisance.

I didn't know about the change in California law making the DL primary id. The fake driver's license didn't have correct versions of my name, my birthdate, or my signature (all things the bank could have checked, but didn't). The gang didn't have my preprinted deposit forms, so they hand-wrote my account number on counter forms. But they didn't take quite \$1,000 at a time and did it all in one banking day at multiple branches distant from my home branch, so apparently didn't trigger any real-time validation. Offline validation did bring in the fraud department. The bank notified me of the problem, rather than vice versa. As far as I know, the gang never tried again using my new accounts.

Jim H.

---

**✶ Re: Serious new CA Drivers License ID RISK (Cornell, [RISKS-21.29](#))**

"John Rickenbrode" <rickenbrode@home.com>  
*Mon, 26 Mar 2001 22:52:38 -0800*

(really about Cal. Commercial Code section 4406)

While Mr. Cornell's concerns ([RISKS-21.29](#)) about the CA driver's license may be well-founded, his message's partial quote of California

## Commercial Code

section 4406(d) leaves out important parts of the statute.

Cal. Com. Code 4406 provides a "safe harbor" to banks to allocate losses from forgery onto customers who do not promptly report unauthorized transactions on their account. So long as a bank provides its customers with sufficiently detailed statement of account, the subdivisions of section 4406(a-c), which were not quoted in Mr. Cornell's message, create a duty upon a bank customer to "exercise reasonable promptness" in examining their bank statements to locate, and report, unauthorized transactions. If the customer does not do this, the customer has not exercised ordinary care, and thus, between the customer and the bank, the customer must bear the loss.

However, the quoted section (d) provides an additional protection for a customer, even when failing in this duty, if the customer can prove that the bank was also negligent in accepting the forgeries. In that case, subdivision (e), a comparative negligence standard (e.g. customer 20% responsible, bank 80% responsible), is used to apportion the loss.

This is not a new law. It was initially adopted in CA in 1965 as part of the Uniform Commercial Code. A 1992 revision increased the time period of subdivision (d)(2) from 14 to 30 days (which only fully applies when the same wrongdoer makes successive transactions). The UCC section was itself derived from prior statutes and case law concerning the allocation of loss from forgery and a customer's duty to provide notice of

unauthorized  
transactions.

Source: Cal. Com. Code Section 4406 (Deering 2001).

The important point, which was not clear in Mr. Cornell's message, is that if you don't promptly check your bank statement for unauthorized transactions (and report any to your bank), you, not the bank, can be forced to suffer the loss.

If you do suffer substantial losses from forgery, which your bank tries to stick on you, reading the unannotated versions of statutes available on the web are probably not going to constitute winning legal research: get a lawyer.

I am not a lawyer. This information is presented for discussion purposes only, not as legal advice.

John Rickenbrode <rickenbrode@home.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 21: Issue 33**

**Sunday 8 April 2001**

## Contents

- [Software direct cause of December 2000 Osprey crash](#)  
[Peter B. Ladkin](#)
- [Computer cords used in escape from police custody](#)  
[Ulf Lindqvist](#)
- [WRQ/Reflection and DST](#)  
[Marc W. Mengel](#)
- [Dutch government report on privacy](#)  
[Peter Fokker](#)
- [Proposed "open" development of voter data standards launched](#)  
[David Marston](#)
- [Re: MS Word: Ohm, SaveAs Watt](#)  
[Markus Peuhkuri](#)
- [Re: Windows 2000 source code](#)  
[Dave Aronson](#)
- [Re: April Fools items](#)  
[Ursula Martin](#)
- [Re: When security is based on trust](#)  
[Ken Cox](#)
- [What's in you server room?](#)  
[Audun Arnesen Nordal](#)

- [Re: tax returns](#)  
[Wendy Grossman](#)  
[Paul Ward](#)
  - [Re: identity theft](#)  
[Chris Viles](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

## ✶ Software direct cause of December 2000 Osprey crash

"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>  
*Sat, 07 Apr 2001 10:25:28 +0200*

Two recent documents have appeared concerning the Osprey, the U. S. Marines' V-22 tiltrotor aircraft intended as the replacement for certain of its aging helicopter fleet. Various problems during Osprey development, including the crash whose cause is related here, have already been reported in [Ladkin et al, [RISKS-21.20](#)].

One document is the U.S. General Accounting Office (GAO) briefing material on its inspection of the Osprey development program, GAO-01-369R "Defense Acquisitions: Readiness of the Marine Corps' V-22 Aircraft for Full-Rate Production", which may be found by searching at <http://www.gao.gov> for term "Osprey" and Keyword "V-22". I highly recommend reading this material to anyone interested in the development of complex systems with crucial computer-based components. It contains some astounding material. I shall not comment further in this note on this document.

The other is the text of the briefing upon release of the JAG report into the cause of the December 2000 Osprey crash during a training mission, at [http://www.defenselink.mil/news/Apr2001/t04052001\\_t405mv22.html](http://www.defenselink.mil/news/Apr2001/t04052001_t405mv22.html) (thanks to Ken Garlington for the link).

First, some details as to how the Osprey functions. It has an engine and a propeller-rotor, bigger than a normal propeller and smaller than a normal helicopter rotor, on the end of each wing. The engine nacelles (structures holding engine and rotors) rotate between roughly vertical (when the aircraft is said to be in "helicopter mode") and horizontal ("airplane mode"). This configuration allows the advantages of a turboprop airplane, such as speed, en-route, but those of a helicopter for take off and landing, and other functions such as loading and offloading personnel and cargo while hovering. This technology has been tested for over twenty years in prototypes such as NASA's XV-15, and the MV-22 is the first attempt at a large production tiltrotor vehicle for use in military missions.

Some words now about flight control. A helicopter rotor has two basic means of adjustment. The angle of the blades can be adjusted relative to the plane of rotation ("pitch"), either uniformly for all blades ("collective pitch"), or differentially in a specific orientation relative to the aircraft body ("cyclic pitch"). This is accomplished by allowing the blades to pivot or flex about their longitudinal axis, and controlling this flexing via rigid connections from the blades to a "swash plate", which is like a

large, loose washer around the rotor spindle back of the rotor. To obtain "collective" control, the swash plate is moved uniformly up and down the spindle to flex the blades together into the desired position. To obtain "cyclic" control, the swash plate is tilted on the spindle in a fixed direction relative to the aircraft body, to produce differential lift in this orientation. An airplane turns by producing differential lift on its wings (by altering their shape via ailerons) but only has two directions in which to do this; the helicopter has full 360-degree freedom in this regard. The third helicopter flight control is the power generated by the engines. In addition, the Osprey has a flight control which consists in rotating the nacelles to various positions between horizontal and a little past the vertical.

Much of the flight control has to be adjusted automatically for the conditions of flight and is not freely controllable by the pilot. It is a "fly-by-wire" (FBW) machine. I find the technology remarkable, and wish it every success, which success no longer appears to be guaranteed, thanks amongst other things to the understanding of the causes, including institutional ones, of the two crashes in 2000.

The briefer, General Berndt, explained what happened in December as follows. The aircraft was flying at about 160kts and the nacelles were transitioning from airplane to helicopter mode. At that point, a flight

control system hydraulic line the left nacelle ruptured under pressure. The nacelle transition was stopped, as per design. These lines are titanium, 22/1000 inch thick, and operate at pressures of 5,000 psi (rather than the more conventional 3,000 psi or so of modern helicopters. Specific requirements other than those of flight control, for example weight and payload requirements, apparently necessitate this high pressure design). The rupture was caused under loading of the system to operate the swash plate, at a weak point caused by chafing of the line against a wire bundle. (I understand that titanium, whilst light and strong, is also quite brittle.) Such chafing has been noted in maintenance reports since July 1999, and some chafing was found on all remaining Ospreys during post-crash inspection. This is apparently a generic problem that has not yet been solved. The aircraft had been properly maintained, and it was ahead of its maintenance schedule, having completed its 210-hour inspection already by 157 hours, its total time at crash. (General Berndt phrased this as being in "excellent shape", but the aircraft evidently wasn't; I think he must have meant that the aircraft was properly determined to be in "excellent shape" by the maintenance procedures. It is becoming recognised in aviation maintenance circles that the inability to inspect certain regions of wire bundles and other lines often allows some dangerous deterioration to go undetected.)

There are three partially-independent hydraulic systems for flight control. The line that ruptured was common to both the number

one and number three systems at that point. The loss of fluid was rapid; the number one system was taken off-line immediately and a shut-off valve isolated the number three system on that side, rendering it inactive on the left, although it remained active on the right side. The number two system carried on as it should have. This form of partial redundancy likely means that it takes two independent failures to cause a total hydraulic flight control system loss. Losing your flight control is catastrophic; design principles and regulations say there should be no possibility of a single point of failure, so two is minimum. And an independently ruptured number two line at that point would have caused total loss of swash plate control on the left, so it seems that catastrophic failure can indeed be caused by certain combinations of two failures.

The machine was left with one operating hydraulic swash plate control system on one side, and two operating systems on the other, but should have been able to fly normally without discernible disturbance to control.

However, there is a Primary Flight Control System (PFCS) reset button available to the pilots. It illuminates under certain circumstances. When illuminated, it should be pressed, which resets the flight control system computers to a known, "safe" state. It illuminated, the crew pressed it to reset the system. This is intent, design, and correct standard procedure. However, what happened then was unplanned, unforeseen, and uncontrollable. The effect of the reset on the state of the

actual flight controls in these circumstances should have been nothing. It is easy to see this: one has lost a hydraulic system, partially lost another, but one wants to continue without interruption using the remaining "assets" whilst isolated the problem as far as possible, and that happened up to that point according to design plan.

However, "no change" is not what the PFCS computers commanded. They apparently commanded changes in rotor pitch and thrust, which became rapid fluctuations. The crew repeatedly recycled the reset. These flight control changes happen via the swash plate. Because of the reduced control power on one side (pressure from one hydraulic system) compared with the other (pressure from two), the rotors responded at different rates to the rapid command changes, as a matter of mechanics. This caused large fluctuations in flight state, control was lost and the aircraft crashed, from an altitude of around 1,600ft. All this happened inside about 30 seconds. The crew is completely without fault in the accident.

General Berndt noted the JAG team was tasked only with determining the course of events and the immediate causes. He therefore had no comments on other aspects of the program, or how this crash will impact procedures in particular or the program in general.

There are some general points to note. First, the aircraft crashed because of two presumably independent failures: the hydraulic system failure and

then the PFCS command failure. So there is no apparent reason to question the fundamental design principles, which both require two independent failures for catastrophe, and (as we have noted) allow it. Second, the first failure was dealt with as designed. The failed system component was isolated as designed and the remaining systems were able to carry out the designed task. Third, the PFCS command failure, which the JAG team has said is a software failure, was completely unplanned and unexpected. The SW caused a "control excursion" and it should not have. General Berndt has said it is "an anomaly in the control logic in the computer software control laws" which seems as if it would be a design failure. But in response to a question, General Berndt suggested he couldn't actually be that specific.

General Berndt was asked who provided the SW. He said he didn't know.

A member of the audience said that Bell was the primary software provider. He replied "but they may subcontract". According to James

Dao of the New York Times, reporting on 6 April, 2001, the software

was written by BAE Systems (the former British Aerospace) and integrated with the hardware by Boeing. (Thanks to John Rushby for this information.)

Peter B. Ladkin

---

## **✶ Computer cords used in escape from police custody**

Ulf Lindqvist <ulf@sdl.sri.com>

*Sat, 7 Apr 2001 21:02:00 -0700 (PDT)*

From Swedish newspaper \*Aftonbladet\* April 7, 2001,  
<http://www.aftonbladet.se/vss/nyheter/story/0,2789,46262,00.html>

An 18-year old man arrested for kidnapping and several counts of aggravated robbery escaped from his cell by breaking the window open and using computer cords to climb down. He had been placed in solitary confinement because of the risk that he could interfere with the investigation if in contact with other suspects. The isolation affected his mental health, so the officers let him play computer games for recreation. The computer was in the only cell in the jail where the window could be partially opened. The suspect used a chair to force the window open and used the cords from the computer to climb down to the roof of another building. This was the second escape ever from the police jail in central Stockholm, which has been in operation since 1975.

I wonder whether this escape will be marked as a computer-related crime in the statistics?

Translated and edited by  
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/>

---

**✶ WRQ/Reflection and DST**

"Marc W. Mengel" <mengel@fnal.gov>  
*Mon, 02 Apr 2001 12:20:03 -0500 (CDT)*

Here at Fermilab we've been rolling out a Strong Authentication Project, and for Windows NT systems we've been using a package called Reflection from WRQ. This morning, NT users were unable to authenticate to the kerberos key servers unless they disabled the Windows setting to "automatically adjust for daylight savings time". Of course, with this setting off, all the time displays on the system are off by an hour, but users can log in to our secure-realm systems with kerberos.

Note that the Windows2k software that does kerberos directly was apparently not affected, only the third party software for Windows NT.

Marc Mengel <mengel@fnal.gov>

---

## **🚩 Dutch government report on privacy**

Peter Fokker <peter@berestijn.nl>  
*Sat, 31 Mar 2001 14:21:17 +0200 (CEST)*

Dutch government advised to give citizens Web access to 'digital vault' with their personal information.

On 29 Mar 2001, Roger van Boxtel, the Dutch minister responsible for ICT issues, received the first copy of the report prepared by the "Commissie Modernisering van de GBA" (Committee for Modernising the Basic Municipal Civil Registry). The committee's task was to present proposals

to make the Civil Registry more accessible and at the same time give citizens a stronger position in their relationship with the government.

In this report, the committee advises the minister that all citizens should be provided with a personal 'digital vault' which would contain selected personal data, taken from a person's "administrative history" in the Civil Registry, including name, address and SoFi number (SSN). Citizens should be able to add even more information to their vaults, such as financial information or data regarding their health. Selected government agencies, such as the Belastingdienst (IRS) and the police, would be given access to these vaults. It is up to the citizen to give other institutions and/or companies access.

The committee stipulates that no citizen should be forced to actually use the digital vault and that citizens should not be forced by third parties to provide information from the vault.

The digital vault is to be made accessible through the website of the municipality where the citizen resides. In the future, the proposed electronic Dutch Identitycard, with biometric authentication, could be used as the key to unlock the vault.

More information (in Dutch) on Roger van Boxtel's own site:  
<http://www.ministervanboxtel.nl/asp/page.asp?id=i000673&version=nl>

Why do I have the feeling that many RISKS are lurking here?

I have a savings account and a safe to store valuables at a bank of my choice. If I am not satisfied, I select another bank. Why would I want to store valuable personal information in the town hall? How can I be sure that my 'digital vault' is indeed safe and that my safe will not be cracked? How can I be sure that there is no possibility that a third party (a cracker) can take over my vault and hence my identity? How long will it take before such a vault is mandatory? Will I be able to prevent the municipality from creating a vault for me or will they do it anyway?

On the other hand: if ever one of these vaults is cracked and something nasty happens with someone stealing my identity, I can always say it wasn't my vault.

Peter Fokker <peter@berestijn.nl>

---

## **⚡ Proposed "open" development of voter data standards launched**

David Marston <marston@mv.mv.com>

*Thu, 29 Mar 2001 22:59:57 -0500 (EST)*

The Organization for the Advancement of Structured Information Standards (OASIS, <http://www.oasis-open.org>) is starting an effort to standardize an XML vocabulary and related software concerning elections. There could be RISKS of overly free interchange of voter registration data, as well as previously-noted concerns about Internet-based voting. Further,

some may view this as a move by election.com to gain early-entrant advantage that could scare away development of competing technology, but I think the OASIS process promotes competition where it matters. Quoting from the first announcement:

A new OASIS technical committee is being formed. The Election and Voter Services Committee has been proposed by Gregg McGilvray, election.com (chair); Oliver Bell, Microsoft; and Ed McLaughlin, Accenture.

**Purpose:** To develop a standard for the structured interchange of data among hardware, software, and service providers who engage in any aspect of providing election or voter services to public or private organizations.

The services performed for such elections include but are not limited to voter role/membership maintenance (new voter registration, membership and dues collection, change of address tracking, etc.), citizen/membership credentialing, redistricting, requests for absentee/expatriate ballots, election calendaring, logistics management (polling place management), election notification, ballot delivery and tabulation, election results reporting and demographics.

**Implementation:** The standard under development by election.com, Inc. will be made available for review and revision and can be expanded upon as necessary. A phased approach will be used to implement the standard due to the number of aspects being considered by the standard.

David Marston <marston@mv.mv.com>

---

## ✉ Re: MS Word: Ohm, SaveAs Watt

Markus Peuhkuri <puhuri@tct.hut.fi>

27 Mar 2001 12:42:23 +0300

Kevin Rolph <kevin@kgames.demon.co.uk> wrote:

> automagically converted the Omega symbols into 'W's (and not to mention ...

Just to complete list of "for user convenience" "features" of the very same

word mangler .. processor. My wife wrote her doctoral thesis with Word 6.0.

After quite a few rounds of proof reading, it was considered error-free

(later found some :-{). To make it ready for press and on-line publication

it had to be converted to PDF.

The computer which had Acrobat tools had also Word 97, with quite default

settings. The document loaded quite nicely, expect some changes in page

layout. We checked for that and then printed it out, sent to the press and

were satisfied.

Before dissertation, she took a closer look at her thesis and noted that

capitalization of some acronyms of compounds (thesis were about pharmacology) were wrong. In disbelief she checked last printouts from Word

6.0 version, and there they were right.

The only possibility is that the Word processor changed them "automatically"

in converting version. I was aware of correct-when-you-type,

but this was  
new... too late. No warning dialogue, nothing.

Ok, back to plan home automation... for family convince

Markus Peuhkuri ! <http://www.iki.fi/puhuri/>

---

## ✶ Re: Windows 2000 source code (Thorson, [RISKS-21.31](#))

Dave Aronson <postmaster@airnsun.dcfido.org>

*Mon, 02 Apr 2001 17:56:40 -0400*

Suspending disbelief for a moment, let us suppose this WERE true. (For those whose disbelief was already suspended, consider the RISKS of glossing over a spokesperson's name, not remembering certain traditions when April rolls around [Lirpa Loof?], etc.) I'm sure we can all envision it happening, be it to Microslop or some other careless company. Methinks we should consider the effort to remove such things, or the embarrassment resulting from not doing so, to be a RISK of not having coding standards, including commandments to the effect that Thou Shalt Use Meaningful (And Not Embarrassing to the Company) Variable Names -- and CODE REVIEWS to enforce it! Or at least code reviews, conducted by a humorless PHB....

Dave Aronson, Sysop of AirNSun free public Fidonet BBS @ +1-703-319-0714

The above opinions are MINE, ALL MINE, but for rent at reasonable rates.

## ✉ Re: April Fools items ([RISKS-21.31](#))

Ursula Martin <um@dcs.st-and.ac.uk>

*Sun, 1 Apr 2001 20:05:05 +0100*

The foot-and-mouth item is indeed not RISKS-unrelated: it is suggested that some of the spread is due to unrecorded trade in sheep to exploit profitable loopholes in the subsidy regulations.

The Sunday Telegraph had one about new European legislation that threatens impersonators who will have to pay royalties to their victims. "Larip Loof, the Finnish European commissioner, explained that the ruling on individuals owning their own voices was "a logical progression" from the laws covering intellectual property rights."

<http://www.telegraph.co.uk:80/et?ac=000125824864271&rtmo=gjNZZZnu&atmo=gjNZZZnu&pg=/et/01/4/1/nimp01.html>

[URL broken by PGN for readability]

Ursula

---

## ✉ Re: When security is based on trust

"Ken Cox (11359)" <kcc@research.bell-labs.com>

*Tue, 27 Mar 2001 14:42:28 -0600*

Michael Sinz' note on Microsoft's ActiveX certification problem ([RISKS-21.30](#)) prompted me to write of another Microsoft-related

RISK that

I've noticed recently. Microsoft has been running a television commercial for one of their e-commerce servers. As the video shows conveyor belts with packages moving along them, the announcer is saying something like,

"John Smith normally orders books about motorcycle racing and scuba diving.

But today, his order included videos that feature a singing purple

dinosaur. The software quietly updates itself to be ready for John's next order."

Perhaps I am just overly suspicious, but I don't think that

"quietly updates

itself for the next order" is the proper reaction. "Loudly

screams for a

service representative and reports this sudden, possibly fraud-related,

change in buying patterns" would be better.

Speaking of which, \*The New York Times\* reported on 26 Mar 2001 (Business

section) that US patent number 6,185,415 has been issued. This patent

covers a class of fraud-detection algorithms that use a certain type of

profiling to detect unusual behavior. The article says that the patent's

owner, @Comm Corporation, has started to pursue

telecommunications companies

that use such software in their systems.

Ken Cox

kcc@research.bell-labs.com

[Interesting. In my lab we have been doing profile-based anomaly

detection since 1983. PGN]

## ✶ What's in you server room?

Audun Arnesen Nordal <audun@stud.cs.uit.no>

Tue, 27 Mar 2001 11:22:47 +0200 (CEST)

I recently quit my job as a system administrator, but I still read the messages and discussions between my former colleagues to help out the guy that followed me in the position. A few days ago, one of my former colleagues entered the server-room at my former employer and found it filled with light smoke. Not seeing any fire and in doubt of how to handle the situation, he consulted his boss in the neighboring room, who ordered an immediate shutdown of all servers. This might seem like an overreaction, but we had experienced some inexplicable hardware malfunction over the past six months that has caused near catastrophic data losses, so tensions wrt. hardware malfunction was high.

It turned out that it was simply an old vt420 terminal that was practically never used that had started to malfunction and producing smoke, but the immediate shutdown of all servers resulted in the client users with for instance open word documents on the server or whatever they were doing to lose any unsaved data.

The risk of putting non-reliable legacy equipment in the same room as your \$30,000 servers with hundreds of concurrent users is obvious. Such server-rooms should not contain any equipment whose catching fire is irrelevant to the operation of the servers. Alternatively, such

equipment

should be shut off (and perhaps disconnected) when not in use.

Audun Nordal

---

**⚡ Re: Tax returns ([RISKS-21.30](#))**

<wendyg@cix.compulink.co.uk>

27 Mar 2001 10:47:15 GMT

> The IRS expects 42 million electronic returns this year -- 70%  
> of all  
> returns.

How is that possible? 70 percent of households don't even have computers!

[There was an error in the report from which the RISKS item was created.

It seemed strange to me, but it was their error, not mine.  
PGN]

---

**⚡ Re: Tax returns ([RISKS-21.30](#))**

<pasward@styx.uwaterloo.ca>

Tue, 27 Mar 2001 10:39:48 -0500 (EST)

From the IRS Stats website at

[http://www.irs.gov/prod/tax\\_stats/soi/ind\\_agi.html](http://www.irs.gov/prod/tax_stats/soi/ind_agi.html)

I discovered that there were 124,770,662 tax returns filed in 1998 (so much for the 10-1 rule). That would make 42 million around 1/3. If I assume

that the number of filers has gone up, probably the error was that 70% will not use electronic filing.

(I also discovered that it is really hard to read a spread sheet that uses proportional fonts rather than fixed fonts.)

Paul

---

## **✶ Re: identity theft ([RISKS-21.30](#))**

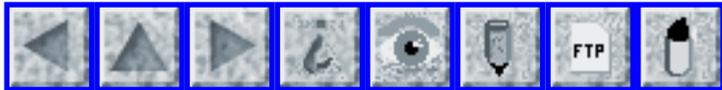
Chris Viles <cviles@swbell.net>  
*Tue, 27 Mar 2001 15:28:58 -0600*

By now, most RISKS readers are familiar with the discount cards that seemingly every supermarket in the US offers. For the small price of a few bits of information you get a discount on your grocery bill every time you buy something from a store in the same chain.

On a recent business trip to the Chicago area, I stopped into a supermarket and was prompted for a discount card as was, I'm sure, everyone else who purchases anything from that chain. Since it's unlikely I'll be back through a store in this chain any time in the near future, I declined their polite offer to "Join and Save". While I gathered my items and prepared to leave, I overheard the clerk ask the person behind me for her card. Unfortunately she had forgotten it, and asked if they could look her up by her phone number. The clerk apologized that no, they no longer

could do  
that and could \*only\* look up by SSN. Which the woman promptly  
rattled off  
for the clerk, myself, and 2 other strangers behind her.

Is your identity worth \$1.45? (The discount I would have  
received if only I  
had "Joined & Saved")



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 21: Issue 34**

**Wednesday 11 April 2001**

## Contents

- [MIT'S cathedral of learning: online and free NewsScan](#)
- [Modern Times, II](#)  
[jhaynes](#)
- [Careful with that e-mail!](#)  
[Lord Wodehouse](#)
- [Risks of appearing in rec.humor.funny](#)  
[Jim Griffith](#)
- [Re: Risks of auto-updating software](#)  
[L. P. Levine](#)
- [More on Yahoo mail's anti-virus attachment translation](#)  
[Kirrily Skud Robert](#)
- [Re: Bogus Microsoft Corporation digital certificates](#)  
[Nick Brown](#)
- [Summertime blues](#)  
[Lord Wodehouse](#)
- [Re: Upcoming time-change risks](#)  
[Derek Ziglar](#)
- [Another Silly Date Problem](#)  
[Peter B. Ladkin](#)

- [Re: Dutch police fight cell theft ...](#)  
[Zygo Blaxell](#)  
[Christian Bartsch](#)
  - [Re: Cellphone text 'bombs'](#)  
[Peter Chuck](#)
  - [Re: Future Mac Viruses?](#)  
[Craig S. Cottingham](#)  
[Paul Hessels](#)
  - [Re: "Internet Voting is no 'Magic Ballot'"](#)  
[Julian White](#)  
[Jay R. Ashworth](#)
  - [Bathtub Burnout](#)  
[Rebecca Mercuri](#)
  - [Auto-updating and ReplayTV](#)  
[Alan Wexelblat](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

## ⚡ MIT'S cathedral of learning: online and free

"NewsScan" <newsscan@newsscan.com>

Wed, 04 Apr 2001 09:05:05 -0700

The Massachusetts Institute of Technology has committed up to \$100 million for a 10-year project to create public Web sites that offer, without charge, learning materials used in almost all of its 2,000 courses. The materials will include lecture notes, problem sets, syllabuses, exams, simulations, and video lectures. Called OpenCourseWare, the program is not intended for "audit" purposes and not as a means for students to earn college credits. Computer science professor Hal Abelson explained: "In the Middle Ages people built cathedrals, where the whole town would get together and

make a thing that's greater than any individual person could do and the society would kind of revel in that. We don't do that as much anymore, but in a sense this is kind of like building a cathedral." MIT President Charles M. Vest is confident that the new program will in no way detract from the value received by residential students who are paying tuition of \$26,000 for the on-campus experience of working directly with faculty and other students." I don't think we are giving away the direct value, by any means, that we give to students. But I think we will help other institutions around the world... I also suspect in this country and throughout the world, a lot of really bright, precocious high school students will find this a great playground." (\*The New York Times\*, 4 Apr 2001; NewsScan Daily, 4 Apr 2001 <http://www.nytimes.com/2001/04/04/technology/04MIT.html>)

[This is a marvelous development to invest in the future. RISKS applauds MIT. Three Cheers! PGN]

---

## **Modern Times, II**

<jhaynes@alumni.uark.edu>

*Sun, 8 Apr 2001 10:13:24 -0500 (CDT)*

The local paper reprinted a column by \*Los Angeles Times\* columnist Doris Kearns Goodwin. She starts out saying that Abe Lincoln's 1861 first inaugural address reached Sacramento in a time of seven days and 17 hours by

Pony Express. "On March 17, [2001] the London Times released a Web version of a story that would appear in the next day's paper, falsely alleging that Steven Spielberg -- who has optioned my unfinished manuscript on Lincoln -- and I planned to present Lincoln as a 'manic depressive racist' and head of a 'dysfunctional' family 'who nearly lost the American Civil War.'"

"Carried by satellite, the story reached Matt Drudge's Florida headquarters and was placed on his Web site even before the newsprint edition of the London Times had reached the streets. In the next 24 hours, 1.6 million hits were recorded on the Drudge site. The story was picked up by dozens of newspapers and made it to Rush Limbaugh's Web site, where Spielberg and I were accused of engaging in a left-wing conspiracy to denigrate American heroes in order to enhance the reputation of Bill Clinton. Within hours, the story was being discussed on talk radio and on television, and I was receiving e-mails from Lincoln scholars as far away as Australia, who were understandably concerned by the story's portrayal of my intentions."

Goes on to say that no reporter ever contacted her to check the accuracy of the story, and that the original reporter blamed the error on others and would allow her to submit a letter to the editor; but by then the false story was all over the world. Goes on to detail some history of Lincoln, some very early statements of his that could be construed to make him appear racist, clearly voided by his later statements, including his last speech,

which stirred up John Wilkes Booth to kill him.

---

## ✶ Careful with that e-mail!

Lord Wodehouse <w0400@ggr.co.uk>

*Fri, 6 Apr 2001 17:54:05 +0100 (GMT Daylight Time)*

Reported by the BBC

[http://news.bbc.co.uk/hi/english/world/americas/newsid\\_1263000/1263917.stm](http://news.bbc.co.uk/hi/english/world/americas/newsid_1263000/1263917.stm)

A chief executive who used an e-mail to threaten his staff with the sack

for being lazy has seen his company's share price collapse after the message appeared on the Internet.

Neal Patterson, head of the Cerner Corporation in Kansas City, USA, had

no idea his private directive to staff would end up being seen by millions of people on the world wide web.

In the three days after the publication of the message, shares in the

healthcare software development company plummeted 22% on the stock market.

It never ceases to amaze me that people armed with a computer and e-mail

completely lose their common sense. However it seems to be the type of

e-mail that should never have been written let alone sent and not by a

senior person in the company. Gerald Ratner built up the family business,

piling it high, selling it cheap and making a fortune out of cut-price jewelry. But a throw-away joke in a speech at the Royal Albert Hall in front of Chancellor Norman Lamont brought his empire crashing down around his ears. (he called a item he sold cr\*p.) With the Internet the inept director can find that it is even easier to ensure that bad news travels faster and further.

---

## ✶ Risks of appearing in rec.humor.funny

<griffith@olagrande.net>

*Thu, 5 Apr 2001 15:34:57 -0500 (CDT)*

In 1994, I had an article appear on rec.humor.funny titled "AOL's cutting edge customer service", in which I related an incident where an AOL representative responded to a complaint by suggesting that the complainant should "telephone the Internet and talk to their tech support people". Since then (and as recently as today), I've been receiving email from AOL users who are somehow convinced that my e-mail address is the AOL customer service address.

Jim

---

## ✶ Re: Risks of auto-updating software

"Prof. L. P. Levine" <levine@blatz.cs.uwm.edu>

*Tue, 3 Apr 2001 12:49:31 -0500 (CDT)*

Graystreak <wex@media.mit.edu> said:

>In his recent (April 2001) AskTog column, Bruce Tognazzini reports on his

>ReplayTV which, one recent day, updated itself to disable a valuable

>feature.

> <http://www.asktog.com/columns/045ReplayTV.html>

I agree with his main point that software that updates itself is a menace

and a problem, but the replay change that was noted in the Tognazzini

posting came and went in about 4 weeks. I noted the change and did not like

it but said nothing. After a few weeks the feature that had been disabled

(a clean pause without ads) reappeared. I must assume that there was a good

deal of noise made by the customer base as RePlay had just scrapped a

revenue source. Good for them.

Customers who don't like a product revision should speak up and even decide

to drop the product. Manufacturers will listen, but we got to talk.

Leonard P. Levine  
Professor, Computer Science  
Milwaukee

e-mail levine@uwm.edu  
University of Wisconsin-

---

## **✶ More on Yahoo mail's anti-virus attachment translation**

Kirrily Skud Robert <skud@infotrope.net>

*Mon, 2 Apr 2001 22:00:13 -0400*

Further to "Yahoo! Mail translates attachments" in [RISKS-21.27](#), I saw the following e-mail on a mailing list which discusses medieval cookery:

From: <xxxxxxxxxxx@yahoo.com>  
Subject: (OT) "Medireview" ???

Does anyone know why certain Web sites and mail servers change the word

"medieval" to "medireview" without any warning? Have I missed something?

Did they change the spelling of the word, and not mail me the notice?

In addition to translating terms like "expression" to "statement" and "eval" to "review" in an attempt to disable potential virus code, it seems that they don't check for word boundaries, so "eval" is translated to "review" even when it's within a word like "medieval".

It's easy to fix this in Perl (for instance), where the programmer would write

```
s/\beval\b/review/g
```

to check for word boundaries.

The RISKS? Firstly, "two wrongs don't make a right." Yahoo's half-baked attempt to fix one problem without adequate thought or testing has caused more problems. Secondly, while the mangling of the word "medieval" on a cookery mailing list may be unimportant, similar mangling occurring to a person's name, address, e-mail address, URL or other important data could have knock-on effects of a much more serious nature.

Addendum: I've just had a report of an actual instance of a mangled e-mail address:

> Someone [...] changed his e-mail address to "cheval" and several of us  
> couldn't get his new address straight because it kept coming up at  
> "chreview". Eventually, we realized what the word actually was, but it  
> took a while.

\*sigh\*

Kirrily "Skud" Robert <http://infotrope.net>

---

## **✶ Re: Bogus Microsoft Corporation digital certificates (Savit, R-21.30)**

BROWN Nick <Nick.BROWN@coe.int>

*Fri, 6 Apr 2001 17:55:18 +0200*

This whole area is reminiscent of, say, nuclear power, or electronic voting, or anything based on Social Security numbers: the technocrats (who do not necessarily have any technical background, even if they are in the private sector) come up with some great scheme that "simply" relies on nobody ever, ever screwing up. (Since most technocrats have never actually done a real job in their lives, they have probably never screwed up either.) This attitude is known in French as "yapuka", short for "il n'y a plus qu'a...", or "it's easy, all you have to do is...".

It "should have been obvious" (that phrase again) that at some point, somebody would screw up and some invalid certificates would slip out. If this had been considered in advance, Microsoft and Verisign would maybe look a bit less like headless chickens right now.

I have a modest proposal: all documentation and marketing material concerning any system which contains any technology whatsoever should, by law, carry the word "probably" in front of each verb describing technical details of the system, and "unless someone screws up" at the end of each sentence describing (claimed) functionality.

Examples:

- "When you click on the icon of the diskette, Microsoft Word will \*probably\* save your work".
- "When you select 'Book now', the system will \*probably\* reserve your ticket".
- "XYZ Backup Manager means you will never lose another file, unless someone screws up".

See how much more accurate this is? Imagine how much happier the world will be without all the disappointment which users feel when the system fails to deliver as promised.

Nick Brown, Strasbourg, France

---

**✶ Summertime blues**

Lord Wodehouse <w0400@ggr.co.uk>

*Tue, 3 Apr 2001 13:18:28 +0100*

It may have already been noted, but in Germany, Deutsche Telekom had problems with their speaking clock over the weekend of 24th/25th March. Users using the alarm service found that on Monday 26th March their call was an hour late, because the system did not advance to daylight savings time.

I expect there were other problems, including the ones where US and UK/Europe companies found that the time difference was one hour more for a week.

John, Global Research IS, GlaxoSmithKline, Medicines Research Centre,  
Gunnels Wood Road, Stevenage SG1 2NY United Kingdom  
+44 1438 76 3222 e-mail: <mailto:w0400@ggr.co.uk> Web: <http://www.gsk.com/>

---

## **Re: Upcoming time-change risks**

"Derek Ziglar" <dziglar@yahoo.com>

*Tue, 3 Apr 2001 21:08:13 -0400*

- > In the USA we change to Daylight Savings Time (spring ahead) ...
- > This year, that also happens to be the first day in April. ...
- > I can see that this confluence is going to cause some amount of confusion,
- > as some people automatically disbelieve any official-seeming announcement

More true that you may think. I may even cause the media to fail to even report such announcements.

In January 1999, a defect in the Microsoft Visual C++ Runtime Libraries was discovered and documented in PC World magazine. Someone had discovered that the time function in the runtime library had an inherent error that it would misapply the Daylight Saving Time setting of Microsoft Windows anytime the daylight savings time went into effect on the first day of the month--like in 2001. The consequence of this bug is that Visual C++ built programs and others that use this same shared library will 'see' the time incorrectly for the first week of the month, then correct itself. Programs on the same computer that don't use this library should see the time correctly.

The risk? Well, I certainly heard no recent alerts that this was to occur! I had no cause to suspect any problem until Sunday morning when my company's servers started misprocessing work because the C++ programs that process our data 'saw' the time one hour differently than SQL Server itself did. A most perplexing situation to debug--when two programs running on the \*same\* computer have a different view of the time!

Sure, Microsoft reports this bug was supposedly fixed in a service patch to the \*compiler\*, But who was responsible for distributing the fixed \*runtime\* components that were distributed with all the applications people had written using that compiler?

As Alan Wexelblat said, how many people would fail to take seriously a problem warning associated with April 1st? Apparently enough that the media completely failed to follow up on this April 1, 2001 risk they had reported over two years ago!

January 1999 article from PC World

<http://www.pcworld.com/resource/printable/article/0,aid,9327,00.asp>

Microsoft Knowledge Base documentation on the problem.

[http://support.microsoft.com/support/kb/articles/Q214/6/61.ASP?](http://support.microsoft.com/support/kb/articles/Q214/6/61.ASP?LN=EN-US&SD=g)

[LN=EN-US&SD=g](http://support.microsoft.com/support/kb/articles/Q214/6/61.ASP?LN=EN-US&SD=g)

[n&FR=0&qry=daylight%20savings&rnk=5&src=DHCS\\_MSPSS\\_gn\\_SRCH&SPR=VCC](http://support.microsoft.com/support/kb/articles/Q214/6/61.ASP?LN=EN-US&SD=g)

Derek Ziglar, Atlanta, Georgia

---

## ✶ Another Silly Date Problem

"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>

*Fri, 06 Apr 2001 09:15:20 +0200*

I have a digital certificate from a well-known german certification authority, trustcenter.de. They informed me on the 9 February that the certificate was about to run out.

Es laeuft am 04/05/01 15:00:42.000 ab.

(It runs out on 04/05/01)

On the 4 April, they said it again:

Ihr [...] Client-Zertifikat mit den folgenden Daten, [...]

gueltig seit: 04/05/00 15:00:42.000, [...]  
nur noch bis zum 04/05/01 15:00:42.000 gueltig ist.

(Your certificate with the following Information [...] valid since 04/05/00 15:00:42.000 ist only valid until 04/05/01 15:00:42.000)

I believed them. I also want this certificate. But this morning at 06.25 local time they informed me:

Ihr Class 1 Client-Zertifikat mit den folgenden Daten, [...] ist am 04/05/01 15:00:42.000 abgelaufen.

(Your certificate with the following Information [...] ran out on 04/05/01 15:00:42.000)

In the language in which this security agency is writing to me, 04/05/01

means unambiguously 4 May 2001. As it does unambiguously all over Europe.

But they obviously meant it to mean the 5 Apr 2001. Can I \*really\* be the first person that has been caught by this mistake?

This goes to show that it's not only NASA that can mix up their units. The solution is probably to insist that agencies which provide an official security function use ISO-standard dates.

Peter Ladkin

---

## 🔥 Re: Dutch police fight cell theft ... (Dzubin, [RISKS-21.32](#))

Zygo Blaxell <[zblaxell@feedme.hungrycats.org](mailto:zblaxell@feedme.hungrycats.org)>  
*Wed, 04 Apr 2001 16:59:54 -0400*

>After a user reports his GSM handset stolen, [...]

Uhhh...I'm not sure what GSM is in this context, but if it's a misspelling of "GSM", then I see a problem.

In GSM, there is a separate SIM card in the handset which contains all of the subscriber's authentication/authorization information, and which is intentionally interchangeable between handsets (subject to some restrictions, but generally when switching between handsets supplied by the same service provider).

If someone was trying to sell the \_handset\_, they could do so without including the SIM card--I've done this a couple of times as handset technology evolves over the years. The buyer provides their own smart card, and the telco doesn't even have to be informed that the sale took place for the handset to work for its new owner.

Naive GSM users reading this article might attempt to send such messages to their own phone number if their handset is stolen. This won't work if the thief has any clue at all. Kids, don't try this at home.

I suppose it is possible that the police may use the telco's resources to track the handset down by its IMEI or something--handsets, high-end accessories, even batteries these days have serial numbers embedded into them which are accessible from the handset firmware and can be interrogated from the telco (if not routinely broadcast while the handset is on).

Zygo Blaxell (Laptop) <zblaxell@feedme.hungrycats.org>

## **✂ SMS in Netherlands on stolen phones (Re: [RISKS-21.32](#))**

Christian Bartsch <cbartsch@gmx.de>

*03 Apr 2001 00:00:00 +0000*

I've only seen reports (but no firsthand source, maybe because of my lack of the Dutch language), but I have a little difficulty believing them.

AFAIK the SMS service in the GSM network addresses the SIM card in the phone (i.e. the mobile's number). If you insert another (not stolen) SIM card and throw away the old one, you won't receive any text messages. Why? That would require addressing the IMEI of the stolen phone, which to my knowledge is not possible. I think some American phones have their number hardcoded in the phone, but here (i.e. GSM in Europe) you could only annoy anyone using a stolen SIM card, not a stolen phone with a "clean" SIM card in, methinks.

Chris

<http://www.zahlungsverkehrsfragen.de/>

---

## **✂ Re: Cellphone text 'bombs'**

Peter Chuck <PChuck@capgemini.nl>

*Tue, 3 Apr 2001 11:26:24 +0200*

The CNN article correctly explains that every mobile device has a built-in serial number (IMEI). Cellphone operators can block all use of a mobile handset based on this IMEI.

Here in Belgium we have one operator that blocks stolen IMEIs and two others that do not (it would cost them money). The result is that all the "new owners" of stolen cellphones are calling via the lazy/cheap operators.

In the Amsterdam scenario, the taxpayers are funding the police to do the work of private cellphone operators.

Peter Chuck, Consultant, Cap Gemini Ernst & Young, Brussels, Belgium.

---

## ✶ Re: Future Mac Viruses? (PC Rescue, [RISKS-21.32](#))

"Craig S. Cottingham" <cottingham@mac.com>

*Mon, 02 Apr 2001 21:17:56 -0500*

> Mac users have been crowing for some time that their system is less prone to  
> viruses than the horrible alternative. Could this be about to change?

First off, any person who claims that Mac OS is less \*susceptible\* to viruses than the "horrible alternative" is mistaken. The greater part of Mac OS's relative dearth of viruses is due to "security through obscurity" -- in

this case, a much smaller developer base. All the tools you need to write code for Mac OS, virulent or not, have been freely available for download from Apple's web site for more than two years.

> "The box contains three installation CDs -- Mac OS X, Mac OS 9.1 and a CD  
> full of developer tools, including the Cocoa programming environment, which  
> is reportedly simple enough for school kids to use."

Secondly, Linux has included, from day one, developer tools simple enough for school kids to use, as evidenced by the number of open source projects started by students. (The most notable example that comes to mind is Napster; I believe its author was a high school student when he created it.) Following that logic, there should be a preponderance of viruses for Linux. Instead, there are, to my knowledge, none. (Worms which exploit security holes in daemons are a horse -- a Trojan horse? -- of a different color.)

The security model built into Linux and other Unix-like operating systems -- of which BSD, on which Mac OS X is built, is one -- contrasts sharply with the security model, such as it is, built into the variants of Windows. So right from the start, Mac OS X is starting from ground more solid than either its predecessor or that "horrible alternative."

What remains to be seen is how well Apple has balanced the Unix-like security model with the expectations of a user base that is used to having free run of the machine. I haven't installed Mac OS X on any of my machines

yet, but it appears from the posts to one OS X mailing list that the security model is obvious for tasks which require superuser rights.

Craig S. Cottingham <cottingham@mac.com>  
<http://pgp.ai.mit.edu:11371/pks/lookup?op=get&search=0xA2FFBE41>>

---

## ✶ Re: Future Mac Viruses? (PC Rescue, [RISKS-21.32](#))

<hesselp@ashaman.dhs.org>  
*Wed, 4 Apr 2001 16:12:23 -0400 (EDT)*

>Mac users have been crowing for some time that their system is  
>less prone to viruses than the horrible alternative. Could this  
>be about to change?

Considering Mac OS X is running FreeBSD, I don't expect virii to be any MORE of a problem than from their legacy OS. Its pretty hard to write a virus that trashes a whole FreeBSD system.

I don't expect that having an IDE that is so easy kids can use will make any noticeable difference...

Now worms on the other hand.....

Paul

---

## ✶ Re: "Internet Voting is no 'Magic Ballot'" (Ashworth, [RISKS-21.32](#))

"Julian White" <JWhite@Nu-D.com>

*Tue, 3 Apr 2001 09:35:39 +0100*

I must agree with Jay on this one. Ensuring that the Internet vote originates from who it claims to be is not wholly solvable at this time. To many issues around the security of this information (whether that be originality, transmission or storage) make it too risky to implement for such an important process. Also, the flip side of adding complex security is that if the Government were able to validate a vote against a voter, they then will have the ability to collect information on a voter's voting habit. I suspect that this is something that many of us would find unacceptable behaviour on behalf of our esteemed Government staff. For those of us with data protection and/or privacy laws we would at least have legislation to strangle the Government with, for those of you without there will not be much you could do to stop it.

However this does not mean we should exclude "electronic" voting. One can see the advantages of collecting the voting information electronically direct from the ballot box. Replacing the paper based system with an electronic counter would produce a more accurate result, faster. The verification of the voter is done as per normal, by turning up to the ballot station. Of course we need to ensure that the voting tallies are not tampered with, which is probably more procedural than technical.

The critical issues with electronic voting are those as

described by Jurek Kirakowski [[RISKS-21.32](#)], namely the user interface. This will be an issue for the technical, social and psychologist arenas to solve as a collective.

Julian White, Nu-Dimensions, UK. [JWhite@Nu-D.com](mailto:JWhite@Nu-D.com)

---

## ✶ Re: "Internet Voting is no 'Magic Ballot'" ([RISKS-21.32](#))

"Jay R. Ashworth" <[jra@baylink.com](mailto:jra@baylink.com)>

*Tue, 3 Apr 2001 05:16:15 -0400*

Another method of counting can certainly be \*added\* to "paper"... but note what I said about "a physical object that the voter can inspect".

And that can \*be\* recounted; the more important issue. Paper cannot be abandoned. Merely augmented.

Jay R. Ashworth <[jra@baylink.com](mailto:jra@baylink.com)> Baylink The Suncoast Freenet, Tampa Bay FL

<http://baylink.pitas.com> +1 727 804 5015

---

## ✶ Bathtub Burnout (Re: Nordal, [RISKS-21.33](#))

Rebecca Mercuri <[mercuri@gradient.cis.upenn.edu](mailto:mercuri@gradient.cis.upenn.edu)>

*Tue, 10 Apr 2001 22:00:44 -0400 (EDT)*

> The risk of putting non-reliable legacy equipment in the same room

> as your \$30,000 servers with hundreds of concurrent users is

obvious.

Audun Nordal's conclusion is a tad misleading. Anyone who has taken a reliability engineering course (do they still teach such things anywhere?) knows that the "bathtub curve function" indicates that it is at BOTH ends of the equipment age spectrum where the increased possibility of breakdown exists. New equipment burn-in (note the full meaning of this terminology) eliminates many of the front-end problems, but I'd suspect that brand-new \$30,000 servers (with defective CRT monitors) probably are at least as risky as the workhorse VT420s.

Rebecca Mercuri

---

## ⚡ Auto-updating and ReplayTV

Graystreak <wex@media.mit.edu>

*Thu, 5 Apr 2001 08:34:11 -0400*

It has been pointed out to me that Tog's column, which I referenced in [RISKS-21.32](#) is (4) months out of date. The malfeature Tog talks about was removed, apparently, last December.

That does not, I think, obviate my major point. I was not trying to say:

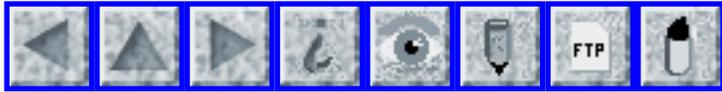
"ReplayTV is bad"

but rather

"we have opened ourselves up to a whole new class of risks" through a combination of always-on/always-connected computers, and auto-updating software.

Risks Digest is a fine forum for presentation and analysis of specific cases; however, part of the point of such cases - I think - is to illustrate larger classes of risks and systemic design flaws which can lead to multiple vulnerabilities.

Alan Wexelblat wex@media.mit.edu <http://wex.www.media.mit.edu/people/wex/>  
moderator, rec.arts.sf.reviews



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 21: Issue 35**

**Monday 23 April 2001**

## Contents

- [Reliance on Automation "Top Risk"](#)  
[Peter B. Ladkin](#)
- [Kew Public Records Office data input problem](#)  
[Pete Mellor](#)
- [Never rely entirely on technology...](#)  
[Peter Houppermans](#)
- [You've Got Mail ... From The Admissions Office!](#)  
[David Tarabar](#)
- [Server 54, Where Are You?](#)  
[Jack Burke](#)
- [Hi-tech toilet swallows woman](#)  
[Gareth Randell](#)
- [Denial of Tax Service](#)  
[Rebecca Mercuri](#)
- [E-mail address ID theft](#)  
[A.E. Brain](#)
- [Sabotaged phone lines + stolen credit cards = safety in theft](#)  
[Simon Carter](#)
- [Security flaw found in Alcatel's high-speed modems](#)  
[Monty Solomon](#)

- [Alcatel admits more than they meant to](#)  
[Mike Bristow](#)
  - [Web-enabled air conditioners](#)  
[Alpha Lau](#)
  - [Risks of sorting time alphabetically](#)  
[Marcos H. Woehrmann](#)
  - [Using Palm VII's to give traffic tickets](#)  
[Ian Jordan](#)
  - [More on UCITA](#)  
[Warren Pearce](#)
  - [Re: Aasta Train Crash](#)  
[Magne Mandt](#)  
[Merlyn Kline](#)
  - [Re: Risks of Hidden highway robbery ...](#)  
[Will Fletcher](#)
  - [Viewers lament incredible shrinking Ultimate TV](#)  
[Monty Solomon](#)
  - [Do prescription records stay private when pharmacy stores are sold?](#)  
[Monty Solomon](#)
  - [New flashlight sees through doors as well as windows](#)  
[Monty Solomon](#)
  - [Windows patchwork](#)  
[Jay Levitt](#)
  - [REVIEW: "Securing Windows NT/2000 Servers for the Internet", Norberg](#)  
[Rob Slade](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

## ⚡ **Reliance on Automation "Top Risk"**

"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>

*Tue, 17 Apr 2001 11:52:59 +0200*

David Learmount, reporting from the Flight Safety Foundation's European Aviation Safety Seminar, held in March in Amsterdam, says in

\*Flight

International\* (20-26 Mar, 2001, p17) that the European Joint Aviation Authorities' Future Aviation Safety Team has identified "crew reliance on cockpit automation" as the top potential safety risk in future aircraft.

PBL

---

## ✂ Kew Public Records Office data input problem

Pete Mellor <pm@csr.city.ac.uk>

Mon, 9 Apr 2001 11:50:40 +0100 (BST)

From Private Eye 6-19th April 2001, p6:

Managers at the Public Records Office in Kew have devised a clever

money-saving idea: they are using prisoners in British jails to input on

to computer the information from the 1901 census. The prisoners' work has

been checked, however, and they have been found to be rewriting history.

All references to prison wardens in 1901 have been changed to "bastards".

Officials are now using cheap labour in India to correct the errors.

Peter Mellor, Centre for Software Reliability, City University, London EC1V 0HB +44 (0)20 7477 8422 Pete Mellor <p.mellor@csr.city.ac.uk>

[And of course no one in India still remembers the British.  
PGN]

## **⚡ Never rely entirely on technology...**

Peter Houppermans <Peter.Houppermans@paconsulting.com>

*Wed, 18 Apr 2001 15:36:29 +0100*

The RISK here is that there appeared to be no inside escape override for the door: taking protection against vandalism to new heights.

<http://www.theregister.co.uk/content/28/18312.html>

Interesting related fact: in the UK, all lift escape hatches are welded shut

(i.e., don't exist anymore in a usable fashion), I vaguely remember that

this was to prevent kids in estate buildings getting themselves in danger in

the elevator shaft (which happened frequently). The fact that this thus

prevents any escape in case of emergency appears to have made insufficient

impact on the decision.

Peter Houppermans <peter.houppermans@paconsulting.com>

---

## **⚡ You've Got Mail ... From The Admissions Office!**

David Tarabar <dtarabar@acm.org>

*Mon, 9 Apr 2001 16:08:03 -0400*

For college-bound seniors, it is a ritual of spring to eagerly await the

daily mail delivery - looking for a thick or thin envelope which will notify

them of college acceptance or rejection.

But for the 94% of applicants to Tufts University, who provided an address, notification of acceptance AND rejection came via an e-mail this year. Tufts follows up with a physical mailing - and thus will reject people twice!

[Boston Globe. 06-APR-2001. "For some, bad news traveling faster"]

Tufts started email notifications several years ago to students in foreign countries. Two years ago it started e-mail notifications to applicants on the West Coast. (Tufts is in Medford, MA) This year it is almost everyone.

The story notes that several colleges have password-protected web sites where an applicant can look up their admissions status.

## Risks

1) This seems impersonal for those who are accepted. It would be interesting to find out if this type of notification changed the percentage who choose to enroll at Tufts.

And it is adding to insult to injury to reject an applicant twice. Tufts must get some very interesting e-mail replies.

2) Not all high school seniors have private email accounts, they are often shared with family members or friends. Thus the wrong person might get the message.

3) Could these e-mails be mistaken for spam? I must get a half dozen offers of University Diplomas each week.

4) Hacking! I shudder to think what could happen if there was a

dedicated  
hacking attack that sent out forged admission e-mails.

---

## ✶ Server 54, Where Are You?

Jack Burke <jfb3@mindspring.com>  
Sat, 14 Apr 2001 08:45:43 -0400

My mind boggles.

The University of North Carolina has finally found a network server that, although missing for four years, hasn't missed a packet in all that time. Try as they might, university administrators couldn't find the server. Working with Novell Inc., IT workers tracked it down by meticulously following cable until they literally ran into a wall. The server had been mistakenly sealed behind drywall by maintenance workers.

Source: TechWeb News, 04/09/01:

<http://www.techweb.com/wire/story/TWB20010409S0012>

This sounds like a novel way -- pun intended -- to physically secure a server. I suppose if you absolutely can't do without a floppy drive, etc., per the Orange book, this might be an acceptable alternative to help meet C2 specifications.

[Except that electronically, it is C-Through rather than C-2.  
[Also noted by Mike Hogsett. PGN]

---

## **Hi-tech toilet swallows woman**

<Gareth Randell>

*Tue, 17 Apr 2001 16:45:30 +0100*

[Source: Article by Lester Haines, 17 Apr 2001, via Brian Randell

<http://www.theregister.co.uk/content/28/18312.html>]

A 51-year-old woman was subjected to a harrowing two-hour ordeal [on 16 Apr 2001] when she was imprisoned in a hi-tech public convenience. Maureen Shotton, from Whitley Bay, was captured by the maverick cyberloot during a shopping trip to Newcastle-upon-Tyne. The toilet, which boasts state-of-the-art electronic auto-flush and door sensors, steadfastly refused to release Maureen, and further resisted attempts by passers-by to force the door. Maureen was finally liberated when the fire brigade ripped the roof off the cantankerous crapper. Maureen's terrifying experience confirms that it is a short step from belligerent bogs to Terminator-style cyborgs hunting down and exterminating mankind.

---

## **Denial of Tax Service**

Rebecca Mercuri <mercuri@gradient.cis.upenn.edu>

*Wed, 18 Apr 2001 14:54:12 -0400 (EDT)*

KYW News Radio in Philadelphia reported on 17 Apr 2001 that there had been a problem when tax procrastinators attempted to file their Pennsylvania State

returns just before the midnight Monday deadline. Apparently in the last few hours, users received an error message from the filing Web site, and they were unable to complete their transaction. Because of this, the state decided to give ALL late filers an extension through 18 Apr. Officials were quoted as saying that "a glitch on the Web server" was the cause of the problem (whatever that means). This brings to mind the possibility of denial-of-service attacks on the infrastructure being a way to avoid paying taxes (short term, anyway).

Rebecca Mercuri

[Life, death, and taxes are not the only sure things. But perhaps

\*electronic\* files could provide a new way to get out of jail. PGN]

---

## **✶ E-mail address ID theft**

<aebrain@dynamite.com.au>

*Mon, 9 Apr 101 11:05:41 GMT*

RISK: The simplest ID theft is that of an e-mail address.

I use e-mail quite a lot for business purposes, and also make regular contributions to a lot of newsgroups. I've been on the net for a decade, so am on a zillion and one "40 million e-mail addresses for just \$5" lists - thank god for filters.

But on Sunday some insufferable person or organisation forged my e-mail address as the sender of some X-rated Spam. This has caused me lost business, a little personal embarrassment, and a mailbox rapidly filling up with bounces from nonexistent addresses. I'm expecting DOS counter-attacks from clueless newbies.

There's not a lot that can be done to stop someone from doing this.

But the risk is that I might not be able to do anything about it in the way of compensation. NeoTrace has given me plenty of clues to the perpetrators, but only by tracing the site that was advertised in the email. Proving it is another matter, and they may have no assets anyway.

A.E.Brain <aebrain@dynamite.com.au>

---

## **✶ Sabotaged phone lines + stolen credit cards = safety in theft**

Simon Carter <smjc@svrc.uq.edu.au>

*Sun, 15 Apr 2001 16:41:32 +0000*

Sabotaged phone lines and stolen credit cards allowed thieves to safely rob a Sydney shopping centre.

"The thieves first sabotaged the telecommunication network in late February. They entered the pits via street-level manholes and severed all the lines leading to shopping centre businesses. With all on-line transaction systems down, shopkeepers processed transactions

manually

and the thieves used stolen credit cards to buy goods and withdraw cash.

Bills are still coming in from the spree."

Full story at <http://www.smh.com.au/news/0104/15/text/national12.html>

Simon Carter

---

## **Security flaw found in Alcatel's high-speed modems**

Monty Solomon <monty@roscom.com>

*Wed, 11 Apr 2001 17:06:38 -0400*

Security flaw found in Alcatel's high-speed modems, By Tim Nott

It's a security flaw. No, it's a spy. No, it doesn't exist at all. Tsutomu

Shimomura, better known for his contribution to, and book about, the arrest

of hacker Kevin Mitnick claims to have found a "trapdoor" in Alcatel ADSL

modems. On Monday evening, Liberation reported, Shimomura and San Diego

Supercomputer Centre colleague Thomas Perrine reported their findings to the

Computer Emergency Response Team. The point, continued Liberation, is

simple. Anyone can penetrate a computer system linked to the Internet by

Alcatel 1000 ADSL and Speed Touch Home modems.

<http://www.thestandardeurope.com/article/display/0,1151,16251,00.html>

## ✂ Alcatel admits more than they meant to

Mike Bristow <mike@urgle.com>

Tue, 17 Apr 2001 16:47:45 +0100

Recently, Alcatel <URL:<http://www.alcatel.com>> has come under fire for security problems with some of it's products (see [broken URL] <<http://www.securityfocus.com/frames/?content=/templates/archive.pike%3Ffromthread%3D0%26threads%3D0%26list%3D1%26end%3D2001-04-14%26mid%3D175229%26start%3D2001-04-08%26>> for details)

As a result, Alcatel has released a statement, as a Microsoft Word document, which they placed on their Web site.

According to <URL:<http://morons.org/articles/1/188>>, it had all the document history present (I cannot confirm this, as they appear to have corrected the mistake), in which we see such gems as:

> (When and where will the firewall software be available? CERT has  
> said that they don't believe that installing a firewall is the  
> answer. What are you doing to provide a legitimate fix?)

The RISKS? Well, apart from looking like idiots, and revealing early drafts of statements that are "off message", and potentially drawing attention to errors of omission that you are conveniently brushing under the carpet...

Mike Bristow, seebitwopie

## Web-enabled air conditioners

=?iso-8859-1?q?Alpha=20Lau?= <avlxyz@yahoo.com>

Mon, 9 Apr 2001 10:38:34 -0700 (PDT)

Not bad! :) Imagine the malicious freezer viruses!

IBM and Carrier, an air-conditioning manufacturer, said they plan to offer Web-enabled air conditioners in Europe this summer that can be controlled wirelessly. Financial terms of the collaboration were not disclosed. Owners of the newfangled air conditioners will be able to set temperatures or switch the units on or off wirelessly using a website called Myappliance.com. <http://www.wired.com/news/business/0,1367,42918,00.html>

From their press release (<http://myappliance.com/myapp/press.htm>): Unit

performance and maintenance information over time can be gathered and

recorded. ... In the opposite direction it is envisaged that Carrier

dealers or engineers will be given 'service access' to check the system

without the need for a PC connection.

In the extreme case, someone with the correct hardware could check the aircond logs to see the typical times the aircond is off, i.e., when no one is home!

Alpha

---

## ⚡ Risks of sorting time alphabetically

<marcos@panix.com>

*Tue, 10 Apr 2001 14:56:38 -0400 (EDT)*

I found a sorting error on Northwest Airlines web site (nwa.com) that I had not seen before, but am surprised is not more common.

If you ask for a list of flights between two cities it returns the

results sorted by departure time of the outbound flight. For example, from San Francisco (SFO) to Minneapolis (MSP) (return flight and other non-relevant data discarded):

Departs	Arrives	Flight Number
6:25am	12:04pm	NW928
7:50am	1:28pm	NW344
10:15am	3:47pm	NW350
11:30am	5:16pm	NW588
12:40am	6:09am	NW360
3:25pm	9:01pm	NW354
5:00pm	10:31pm	NW358

The risk? Assuming that because 11:30am is later than 10:15 am it follows that 12:40am is later than 11:30am.

Another good reason to drop AM/PM in favor of a 24 hour clock (particularly if you call midnight 0.00 and not 24.00).

Marcos H. Woehrmann | marcos@panix.com | <http://members.home.com/marcos>

---

## ⚡ Using Palm VII's to give traffic tickets

"Ian Jordan" <ian@twingles.com>

*Fri, 6 Apr 2001 14:05:26 -0700*

The Seattle news played a story on a local police force that is now using Palm VII's to give traffic tickets. Apparently, officers can look up information on vehicles and people via the wireless interface from this Palm. The obvious risk comes from the publicly based network that the Palm relies on, namely the CDPD network.

Just imagine someone getting a ticket, and wanting to cover it up. If they broke into the system, they could start issuing tickets to every car on the road. How would anyone know what tickets were valid? Simpler security risks also are involved, such as just monitoring the communications and seeing what people are accused of, or even looking for addresses that are transmitted- if someone is getting pulled over, they're probably not home.

As a side note, I wonder how you get your court summons, since this procedure removes paper tickets. It would also appear to eliminate the officer's signature, making for a dubious case, since there is no official document indicating the charge against you.

The full story is linked at:

<http://www.king5.com/biztech/storydetail.html?StoryID=17028>

---

## More on UCITA

"Pearce, Warren, CTR" <Warren.Pearce-contractor@jntf.osd.mil>  
*Wed, 18 Apr 2001 11:50:49 -0600*

Ed Foster's Gripeline column in the current issue of \*InfoWorld\* (www.infoworld.com) raises another interesting security related issue. The column starts with:

Microsoft recently prevented an independent lab from publishing benchmark results, using a term in the SQL Server license that says the user "may not disclose the results of any benchmark test without Microsoft's prior written approval" to threaten the lab with legal action.

It's not my intent to focus on Microsoft as this is an element of UCITA. In prior columns, Ed included a similar comment from Network Associates.

Consider a security related "benchmark test" that reveals a vulnerability.

The vendor's permission will be required to "disclose the results" of the test. What does this do to the entire CERT process?

---

## ✶ Re: Aasta Train Crash

"Mandt, Magne" <Magne.Mandt@ffi.no>

*Tue, 3 Apr 2001 08:10:56 +0200*

There is one very important point that has been forgotten in the latest postings about the fatal Aasta train crash: The railways deliberately introduced a single point of failure system some months prior to the accident. The old operating procedure was that both the train driver and the ticket taker (conductor) had to verify that the signal was green before

the train left the station. Under the new procedure, introduced some months before the crash, only the driver had to check the signal. The line where the crash occurred does not have an automatic train stop system that stops trains that are headed towards each other on the same track, so the drivers observation of the signal is the final barrier against a crash.

Magne Mandt

---

**✉ Re: Aasta train crash (Smorgrav, [RISKS-21.32](#))**

"Merlyn Kline" <merlyn@zynet.net>

*Tue, 3 Apr 2001 11:14:11 +0100*

Am I missing something here or is all this beside the point?  
Using mobile 'phones as a safety-critical means of communication entails so many risks I hardly know where to start: The network coverage is patchy at best and hardly at its best when used in a train; the handset batteries have short lives and are liable to fail; the handsets are easily lost or damaged; handsets are typically unsuitable for noisy environments; communication is dependent on a network outside the control of the train company; even if you get network coverage, cell capacity is limited; the list just goes on and on. Some of these risks can be addressed but some simply cannot. Surely this can't be right?

Merlyn Kline

---

## ✉ **Re: Risks of Hidden highway robbery ... ([RISKS-21.32](#))**

"Will Fletcher" <Will\_Fletcher@msn.com>

*Thu, 19 Apr 2001 20:37:15 -0500*

In [RISKS-21.32](#) it was noted that Microsoft was being particularly heavy-handed with the end-user agreement and the rights to intellectual property transmitted over their.NET or Hailstorm passport service. Wanting to see the fine print for myself I downloaded the agreement at <http://www.passport.com/Consumer/TermsOfUse.asp>. Yes, it does say that Microsoft reserves the right to take advantage of any intellectual property. However, it would appear that the intent of the agreement is allow Microsoft the rights to any intellectual property submitted to them concerning the service, not intellectual property transmitted over the service. Towards the end of the section in question the following appears:

This section also is inapplicable to any documents, information, or other data that you upload,transmit or otherwise submit to or through any Passport-Enabled Properties. Please refer to the terms and conditions for such Passport-Enabled Properties to determine the rights of the web site or service provider to such documents, information and/or data.

The first sentence would seem to limit the rights of Microsoft with respect to misappropriating intellectual property transmitted via these

services. But, then again the second sentence might lead one to be suspicious about how such rights are determined.

Perhaps the real risk is not being able to read all of the fine print, since it is not clear where one would go to find these additional "terms and conditions for such Passport-Enabled Properties".

Will Fletcher <will\_fletcher@msn.com>

---

## **⚡ Viewers lament incredible shrinking Ultimate TV**

Monty Solomon <monty@roscom.com>

*Wed, 18 Apr 2001 01:40:16 -0400*

UltimateTV shrinks from the spotlight

A software bug is inadvertently shrinking hard-drive storage space on set-top boxes for UltimateTV, the new interactive TV service from Microsoft.

The bug reduces how many hours of programming people can record onto the hard drive of UltimateTV set-top boxes. Customers began reporting the problem on Web forums earlier this month.

<http://www.zdnet.com/zdnn/stories/news/0,4586,5081102,00.html>

---

## **⚡ Do prescription records stay private when pharmacy stores are sold?**

Monty Solomon <monty@roscom.com>

*Wed, 11 Apr 2001 17:02:53 -0400*

Do prescription records stay private when pharmacy stores are sold?

The issue caught the attention of the Clinton administration

By Milo Geyelin

THE WALL STREET JOURNAL

April 11 - A novel lawsuit over the privacy of prescription records at a former neighborhood drug store could complicate the way pharmacy chains buy up their competitors. The suit challenges the common but little-known practice of "file buying," in which chains purchase customer prescription files from pharmacies they acquire and add them to their own.

<http://www.msnbc.com/news/557734.asp>

---

## **⚡ New flashlight sees through doors as well as windows**

Monty Solomon <monty@roscom.com>

*Wed, 18 Apr 2001 01:30:46 -0400*

Police officers serving a warrant or searching for a suspect hiding inside a building could soon have a new tool for protecting themselves and finding the "bad guy."

A prototype device called the RADAR Flashlight, developed at the Georgia Tech Research Institute (GTRI), can detect a human's presence through doors and walls up to 8 inches thick.

The device uses a narrow 16-degree radar beam and specialized

signal  
processor to discern respiration and/or movement up to three  
meters  
behind a wall. The device can penetrate even heavy clothing to  
detect  
respiration and movements of as little as a few millimeters.

<http://unisci.com/stories/20012/0416015.htm>

---

## ✶ Windows patchwork

"Jay Levitt" <jay@jay.fm>  
*Tue, 10 Apr 2001 22:09:50 -0400*

A recent \*Wired\* news article  
<<http://www.wired.com/news/technology/0,1282,42771,00.html>>  
detailed  
problems that Microsoft had with an Internet Explorer security  
patch: In  
some cases the patch would wrongly display "This update does not  
need to be  
installed on this system." Although I hadn't seen such a  
message, I  
double-checked that the patch was properly installed - and it  
wasn't. After  
digging further, I was surprised at the reason why.

Microsoft maintains a "Windows Update" site, which automatically  
scans your  
Windows installation (locally), compares it with a list of known  
patches,  
and lists any missing updates. Further, they have a "Critical  
Update  
Notification" tool that runs in the background and automatically  
alerts the  
user when any "critical" patches are added to Windows Update. I  
run the  
notification tool, and I check Windows Update often, so I

expected my system  
to be quite current.

Documentation for the notification tool says: "Download this component and never miss a Critical Update again. Whenever a new Critical Fix is released, you will be notified... Critical Update Notification is the best way to keep your computer up-to-date and protected from potential security issues affecting Microsoft Windows."

As it turns out, although Microsoft puts many of its IE security patches on Windows Update, four critical patches this year were not included there, and thus are not detected by the notification tool. Users must go to a separate IE Security site to download these patches - a site that is not promoted or even mentioned by the Windows Update site or other customer service pages. I first learned of it from the \*Wired\* article.

Risks:

- Maintaining two separate patch repositories
- Promoting a site as the way to "never miss" security patches, but failing to add all security patches there
- Trusting Microsoft to help keep my computer up-to-date

Jay Levitt <jay@jay.fm>

---

## **⚡ REVIEW: "Securing Windows NT/2000 Servers for the Internet", Norberg**

"Rob Slade, doting grandpa of Ryan and Trevor" <rslade@sprint.ca>

*Mon, 16 Apr 2001 08:48:21 -0800*

BKSWN2SI.RVW 20010320

"Securing Windows NT/2000 Servers for the Internet", Stefan Norberg,

2001, 1-56592-768-0, U\$29.95/C\$43.95

%A Stefan Norberg stefan@norberg.org <http://people.hp.se/stnor>

%C 103 Morris Street, Suite A, Sebastopol, CA 95472

%D 2001

%G 1-56592-768-0

%I O'Reilly & Associates, Inc.

%O U\$29.95/C\$43.95 800-998-9938 fax: 707-829-0104 nuts@ora.com

%P 199 p.

%T "Securing Windows NT/2000 Servers for the Internet"

This book is based on the paper "Building a Windows NT bastion host in practice," which is available on the author's Web site. The title of the essay is much more accurate than the title of the text. The work is concerned strictly with bastion hosts, and does not address, in more than a nominal way, considerations of applications that are necessarily part of any Internet server.

Chapter one takes a brief, scattered, and not very clear look at a number of issues related to Windows and/or security. This disregard for background information extends into chapter two. Having presented an extensive list of services to turn off, Norberg tells us that "[you now] understand the purpose of all active software components on the host." The irony of this bald assertion stems from the fact that there has been little discussion of why these services are to be turned off, and what you lose along the way.

(Further, for those new to Windows NT or 2000, there is no indication of how to accomplish the task of reduction.) Once we get into more advanced tuning there is slightly more information, but not much. The material on the differences in Win2K, contained in chapter three, does present a bit more detail on how to accomplish the restrictions.

Chapter four describes a number of software tools that will encrypt sessions to be used for remote administration, but does not deal with system management itself. The standard advice you always read about backups ("make one") is repeated in chapter five. Chapter six reviews auditing and logging, with, for some unknown reason, four times as much space devoted to network time synchronization as to intrusion detection. "Maintaining Your Perimeter Network" is the title of chapter seven, but it seems to be a return to the same kind of catch-all discussion that started the book.

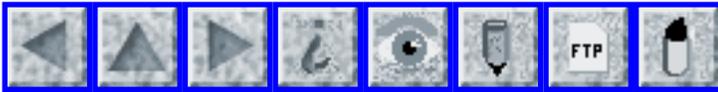
In the Preface, Norberg does state that the book is not intended as a primer for security, or even for Windows security. The text is written as a kind of a checklist for those thoroughly familiar with NT or 2K. There is, of course, nothing wrong with such an approach, and those in the target audience will appreciate the brevity of this concise guide. The approach does, however, severely limit the utility of the work. Chapter two (and three, if you are using Win2K) is the heart of the book, and the rest seems to be an attempt to expand the text to more than pamphlet length.

copyright Robert M. Slade, 2001    BKSWN2SI.RVW    20010320  
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 21: Issue 36**

**Wednesday 25 April 2001**

## Contents

- [Computer system crash stalls D.C. Metro](#)  
[PGN](#)
- [UPS Shutdown](#)  
[Kent Borg](#)
- [Trial by CCTV](#)  
[M Taylor](#)
- [Risks of fabricating funny data](#)  
[Bill Hopkins](#)
- [Foreign Flimflam](#)  
[Keith A Rhodes](#)
- [Wireless Spam](#)  
[NewsScan](#)
- [Slack goes when California DMV gains access to SSA database](#)  
[Elizabeth Weise](#)
- [U.S. Government cyberdefense lacking](#)  
[Dave Stringer-Calvert](#)
- [Errors in AFFX GeneChip Database](#)  
[Gregory Soo](#)
- [35,000-pound hacking challenge cracked](#)  
[Jay Anantharaman](#)

- [Microsoft's wonderful solution for Outlook security](#)  
[Dave Stringer-Calvert](#)
  - [Re: Amtrak 'Sharing' Information With D.E.A.](#)  
[John Noble](#)
  - [Re: Aasta train crash](#)  
[Dag-Erling Smorgrav](#)
  - [Re: V-22: Titanium properties](#)  
[Edwin M. Culver](#)
  - [Bathtub Burnout](#)  
[Jan Verbrueggen](#)
  - [Re: Hidden highway robbery within ... contracts?](#)  
[Norman Gray](#)
  - [Risks of using filtering proxies](#)  
[Marc Roessler](#)
  - [Power safety](#)  
[Marcus L. Rowland](#)
  - [First Workshop on Information Security System Rating and Ranking](#)  
[Jack Holleran](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

## ⚡ Computer system crash stalls D.C. Metro

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

Wed, 25 Apr 2001 07:52:39 -0700 (PDT)

Washington D.C. Metro's \$20 million central computer system crashed at 5:15 p.m. during the evening rush hour on 24 Apr 2001. The central system provides real-time graphics to the downtown control center. Similar malfunctions occurred in 1998 and 1999 (e.g., [RISKS-20.60](#)). In the 15 months following its installation, this BDM system crashed 50 times, according to the Metro. Coincidentally, a six-car train that

had broken  
down 8 minutes earlier was stuck in the tunnel between  
Friendship Heights  
and Bethesda, and had to be towed out.

The outage caused system-wide delays, with some passengers  
facing platform  
delays up to 45 minutes. Fortunately, the automated train  
operation system  
continued working, although manual switching was required, and  
signals  
failed at three junctions (Medical Center, Rosslyn, and L'Enfant  
Plaza).

<http://www.washingtonpost.com/wp-dyn/articles/A60653-2001Apr24.html>

---

## ⚡ UPS Shutdown

Kent Borg <kentborg@borg.org>  
*12 Apr 2001 13:47:57 -0000*

On the evening of 11 April 2001, a fairly large chunk of  
Somerville,  
MA, USA lost power for two-some hours.

I was very smug about having a nice little UPS for my even  
littler basement  
server, and that it ran for nearly two hours before giving me  
its "last  
chance to shutdown" beeps, at which point I did a blind login  
and "shutdown  
-h now". Then I turned on the monitor power, which sent the UPS  
over the  
edge to complete shutown. I left it that way, hard power switch  
on the  
computer still "on" and we went to dinner, me smugly thinking  
the server

would come up with the mains power.

Nope. The Belkin UPS I bought has a soft power switch that doesn't turn on again when power is reapplied. The battery charges, but the UPS power button must be pressed for two-seconds to get power back out back, making this model completely unsuited for unattended operation. I could find nothing in the instructions point out this "feature".

Lesson: Yet another case where having a UPS can be worse than nothing.

Test your systems with someone watching.

-kb, the Kent who is now in the market for a UPS with a simple hard power switch that will stay "on".

---

## **⚡ Trial by CCTV**

M Taylor <mctaylor@privacy.nb.ca>

*Mon, 23 Apr 2001 17:06:52 -0300 (ADT)*

Source: Trial by CCTV claims innocent victim, by Kieren McCarthy  
19 Apr 2001 <<http://www.theregister.co.uk/content/8/18393.html>>

Allan Dunne was arrested, publicly accused of being a criminal, and lost his job because he took 20 pounds out of his own account from a cash machine.

He was caught on CCTV making the transaction shortly just after a thief had used the same cash machine. The footage was shown on Granada TV's Crimefile show. Allan went to the police with records from his own bank

account, but  
was arrested and suspended from his job. Evidence that CCTV is  
not perfect?

---

## ✶ Risks of fabricating funny data

"Bill Hopkins" <whopkins@wmi.com>

*Mon, 23 Apr 2001 16:22:59 -0400*

In 1998, techies at \*The New York Times\* made up amusing capsule  
descriptions for some old movies, with themselves as stars,  
while testing a  
new update path to the TV listing service's database. Contrary  
to  
expectations, the capsules were saved, and when one of the  
movies was  
scheduled, The Times published its bogus description.

Who could have anticipated the movie would be scheduled on 1 Apr  
2001?

Oh, to be a fly on the wall when that went down!

[[www.nytimes.com/2001/04/03/pageoneplus/corrections.html](http://www.nytimes.com/2001/04/03/pageoneplus/corrections.html)]

[Cap-sules rush in where mangles cheer to sched. PGN]

---

## ✶ Foreign Flimflam

"Keith A Rhodes" <RhodesK@GAO.GOV>

*Tue, 27 Feb 2001 08:40:56 -0500*

International thieves are using stolen credit card numbers to  
buy from

U.S. vendors over the Internet. Goods received at U.S. addresses are then being rerouted overseas. One thief had over 300 stolen cards and had purchased \$900,000 in merchandise. On-line credit-card fraud is currently estimated at \$24 million per day. Prosecution is of course complicated by multiple jurisdictions. [Source: Article by Laura Lorek, Interactive Week, 25 Feb 2001; PGN-ed]

---

## ✶ Wireless Spam

"NewsScan" <newsscan@newsscan.com>  
*Mon, 16 Apr 2001 08:00:34 -0700*

The text-messaging services now included as a standard feature by many wireless companies make it simple for senders of junk mail to target a specific audience by geographic location and pass the costs of their messages on to the people being spammed. Todd Bernier, a wireless technology analyst with Morningstar, predicts: "This will become a huge problem when text messages become more popular in the states. The industry is going to have to do something to control itself. People just won't tolerate it."

(AP/\*USA Today\*, 13 Apr 2001; NewsScan Daily, 16 April 2001  
<http://www.usatoday.com/life/cyber/tech/2001-04-13-wireless-spam.htm>

---

## **Slack goes when California DMV gains access to SSA database**

eweise <eweise@usatoday.com>

*Tue, 24 Apr 2001 16:25:02 -0400*

Apparently the California DMV gained access to the computerized database of the Social Security Administration at the beginning of the year. Sometime in February or March the DMV began bouncing back all requests to renew drivers licenses in which the name given did not exactly match the name in the SSA computers.

I learned of this the day my license expired when I attempted to renew it and was told that because my Social Security number was issued under the name Beth back in the 1960s, according to the DMV I was attempting to defraud the government "and possibly engaged in identity theft" by attempting to get a drivers license under the name Elizabeth Weise--despite the fact that the State of California has accorded me a drivers license under that name for eight years now.

A call to the Social Security Administration confirmed that since the DMV was given the ability to hook directly into the SSA's computers, they've been flooded with Robert-Bob's, Richard-Dicks's and Alex-Alexander's who are all being told they can't renew their licenses until they officially change their names. For the record, the clerk at the SSA told me "We understand that Beth and Elizabeth are the same person and it doesn't bother us, but the DMV won't let it by any more." To fix this

one must personally go to an SSA office and have them change their official record.

The identification they require?  
A California drivers license.

Elizabeth Weise, Technology Reporter, USA Today Life Section  
2912 Diamond St. #407, San Francisco CA 94131 415/452-8741  
eweise@usatoday.com

---

## **🔥 U.S. Government cyberdefense lacking**

Dave Stringer-Calvert <dave\_sc@cs.sri.com>

*Thu, 05 Apr 2001 20:03:19 -0700*

U.S. General Accounting Office reviews of 24 agencies (including Treasury, the IRS, and Social Security) reveal that security gaps place ``a broad range of critical operations and assets at risk from fraud, misuse, and disruption.'' During the year 2000, 155 federal computer systems (some with sensitive information) were taken over by unauthorized users who gained full administrative privileges. The military recorded 715 serious attacks in that period. [Source: Study of government computers faults security, by Poornima Gupta, Reuters, 5 Apr 2001; PGN-ed [http://www.siliconvalley.com/docs/news/reuters\\_wire/10531441.htm](http://www.siliconvalley.com/docs/news/reuters_wire/10531441.htm)]

---

## **🔥 Errors in AFX GeneChip Database**

"Gregory Soo hotmail" <grsoo@hotmail.com>

Wed, 7 Mar 2001 20:03:15 -0500

Affymetrix Inc. <http://www.affymetrix.com/> has discovered errors in some of its gene chips, involving the UniGene U74 database used to design its Murine Gene U74 set of GeneChip arrays. The arrays are used to analyze mice tissues and cells. [Source" Affymetrix Discovers Errors in GeneChip Database; GlacierRISKS of database errors propagated into nucleotide-array analysis...  
7 Mar 2001 <http://dowjones.work.com/index.asp> and <http://quote.yahoo.com/>  
PGN-ed]

---

## **✶ 35,000-pound hacking challenge cracked (From Dave Farber's IP)**

Jay Anantharaman <jna@nuance.com>  
Mon, 23 Apr 2001 17:41:15 -0700

A team of computer hackers has gained 35,000 pounds for hacking into a computer system just twenty-four hours after the competition began.

Argus Systems organised the competition -- to break into a Web server locked down using its security product called PitBull -- to promote its products and to coincide with the start of Infosec, the UK's premier computer security event.

Undeniably, the stunt backfired and is an embarrassment for Argus Systems

Group, as well for as security consultant firm Integralis and hardware vendor Fujitsu Siemens, which helped organise the stunt and have coordinated three similar competitions in the US and Germany without suffering setbacks.

[<http://uk.news.yahoo.com/010423/152/bmqfd.html>

From Dave Farber's IP. For Dave's archives, see <http://www.interesting-people.org/> PGN]

---

## Microsoft's wonderful solution for Outlook security

Dave Stringer-Calvert <dave\_sc@csl.sri.com>

*Fri, 06 Apr 2001 11:01:51 -0700*

Microsoft is apparently defending against e-mail viruses (such as Melissa and I Love You) by restricting the types of file attachments that can be opened or downloaded by the newest version of its Outlook 2002, which will reject over 30 types of attachments -- including program execution files, batch files, Windows help files, Java and Visual Basic scripting files, photo CD images, screensavers and HTML application files.

[Source:

Microsoft's virus antidote: Ban attachments, Is Microsoft making the cure

worse than the sickness? by Joe Wilcox, CNET News.com; PGN-ed

<http://dailynews.yahoo.com/h/cn/20010406/tc/>

microsoft\_s\_virus\_antidote\_ban\_attachments\_1.html (URL split)]

[We are getting close to the old days of IBM mainframes (which also had weak -- if nonexistent -- operating system protection), where, in the

absence of RACF or similar security applique, the best advice was not to allow any users, compilers, and especially system programmers on the system -- just canned pre-vetted turnkey application programs. PGN]

---

## ✶ Re: Amtrak 'Sharing' Information With D.E.A. (From Dave Farber's IP)

John Noble <jnoble@dgsys.com>  
*Sun, 15 Apr 2001 18:57:38 -0400*

> Something to think about next time you decide to ride the rails: Amtrak  
> has acknowledged that one of its ticketing offices has been "sharing  
> information" about passengers with the Drug Enforcement Administration,  
> and then taking a 10 percent cut of any assets seized from drug couriers.

It gets better ...

"We provide a limited amount of information about our passengers to the D.E.A. and other agencies as a part of their law enforcement activities," said Debbie Hare, an Amtrak spokeswoman. "I can't tell you how long it has been going on, but this program exists all across the country."

So it's not "one of its ticketing offices," but "all across the country."

"A computer link from Amtrak's ticketing terminal in Albuquerque to the local D.E.A. office allows agents to peruse passengers' names and

itineraries and to see whether they paid in cash or credit. The information determines which passengers will be questioned or have their luggage searched by drug-sniffing dogs."

Names, itineraries, cash/credit. This is profiling. They don't give you a pass when you use a credit card, because then you could beat the surveillance by using a credit card. They can't investigate everybody who pays cash because they don't have the manpower. All they get is a vague indication of wealth and possible preference for anonymity. So they go to names and itineraries -- national origin, race, gender, religion, urban/rural. Now we're cookin'. Maybe they toss in the ticket agent's flag based on his "gut feeling." I wonder if he gets a bonus when he's right.

John Noble

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

Incidentally, apparently Amtrak has just backed off. 25 Apr 2001. PGN]

---

## ✶ Re: Aasta train crash (Kline, [RISKS-21.35](#))

Dag-Erling Smorgrav <des@thinksec.com>  
24 Apr 2001 22:42:43 +0200

Merlyn Kline is assuming that the handsets in question are digital GSM handsets. As far as I know, they're not - they use an older analog system called NMT, which has better audio quality and longer range than

GSM, and better coverage in out-of-the-way parts of Norway. As to battery life, this is hardly a problem on a train, which has plenty of power to spare; and even the most power-hungry GSM handsets have sufficient battery capacity to last a six- or seven-hour shift (the handsets apparently follow the crew).

In any case, this point is moot -- better communications probably wouldn't have made much of a difference in this particular accident; there simply wasn't enough time.

BTW, a few days before my previous article went out on RISKS, the Norwegian Railway Authority (in charge of tracks, station and other infrastructure) was fined NOK 10M (approx. USD 1.1M) for non-adherence to safety regulations. More than a year after the accident, very little has been done to raise the standard of the line where it occurred. The railway authority are whining that the impact of the fine on their budget will delay security work; then again, they've never shown any willingness to to assume responsibility for their own actions in the past, so why start now?

Dag-Erling Smørgrav - des@thinksec.com

---

**✉ Re: V-22: Titanium properties (Ladkin, [RISKS-21.33](#))**

"Edwin M. Culver" <edwin.m.culver@snet.net>  
*Sun, 08 Apr 2001 23:07:17 -0400*

Peter B. Ladkin wrote "...titanium, whilst light and strong, is also quite brittle..."

Before becoming a full time programmer in the early 90's, I was a structural test engineer at a helicopter maker (the one not involved in the Osprey i- ) ).

First, some engineer speak: "brittle" refers to materials which don't exhibit permanent deformation, or set. Glass is an example of a material which is usually brittle.

Titanium-based alloys are light and strong...and not brittle. Or at least not more brittle than the comparable steel or aluminum based aerospace alloys. Most titanium based alloys have better fatigue properties than most steels or aluminum alloys. Titanium has some shortcomings: it can be quite difficult to work (it's flammable), and threads in titanium gall (kind of stick to themselves), but the aerospace industry is quite used to dealing with these.

I'll peruse the GAO articles when I get a chance, but don't really expect any surprises.

While tiltrotor technology is not very new (the original tilt rotor aircraft was built in the 1950's), the V-22 is the first attempt at a production aircraft. It has many problems of both fixed wing aircraft and helicopters and a few that would be unique.

E. M. Culver

---

## ✉ **Bathtub Burnout (Re: Nordal, [RISKS-21.33](#); Mercuri,-21.34)**

"Dr. Jan C. =?iso-8859-1?Q?Vorbr=FCggen?=" <jvorbrueggen@mediasec.de>

*Thu, 12 Apr 2001 13:51:49 +0200*

I actually find both conclusions misleading. The original one was:

> The risk of putting non-reliable legacy equipment in the same room  
> as your \$30,000 servers with hundreds of concurrent users is obvious.

The risk of using systems - hardware and software - that result in unexpected outages leading to the irretrievable loss of data really is the issue here. If the server "went away", why did the users lose their work? It's not that the server's disk actually burnt! - and properly designed systems survive even that (cf. Credit Lyonnais), at a cost, of course. So what really happened? I can still envisage a scenario where shutting down the server incidentally lead to data loss, but from the description provided, I would say the reaction to smoke in the room was quite proper.

Jan Vorbrüggen - MediaSec Technologies, Berliner Platz 6-8, D-45127 Essen  
GERMANY Research & Development +49 201 437 5252 <http://www.mediasec.com>

## ⚡ **Re: Hidden highway robbery within ... contracts? ([RISKS-21.32](#))**

Norman Gray <[norman@astro.gla.ac.uk](mailto:norman@astro.gla.ac.uk)>

*Tue, 17 Apr 2001 13:13:07 +0100 (BST)*

I was rather alarmed to notice that the Yahoo! terms of service [1] (which I would never have looked at without the prompt of this RISKS posting) have an apparently similar licence. However, it refers only to 'publicly accessible areas of the Service', which they explicitly say excludes 'Yahoo services intended for private communication such as Yahoo! Mail' and several other things.

Though I presume that the point of these 'licences' is merely to allow Yahoo to continue to deliver archived postings in future, the licence does go much further than that. The Microsoft version, however, goes further even than the Yahoo one, and doesn't even obviously fail to cover a mail message I might send to a hotmail user.

The RISK, I'm sure, is that you could unwittingly hazard your or your institution's IPR, and be forced to spend time with the local lawyers.

[1] <http://docs.yahoo.com/info/terms/> (section 8)

Norman Gray  
[users/norman/](http://www.astro.gla.ac.uk/users/norman/)

<http://www.astro.gla.ac.uk/>

Physics and Astronomy, University of Glasgow, UK  
[norman@astro.gla.ac.uk](mailto:norman@astro.gla.ac.uk)

## ✶ Risks of using filtering proxies

Marc Roessler <marc@tentacle.franken.de>

Wed, 4 Apr 2001 17:45:49 +0200

In [RISKS-18.65](#) James Cameron wrote about the RISKS of using proxy-servers, as they 'may change your view of the Internet'.

Some days ago I experienced something similar: filtering proxies changing the view of the Internet.

One week ago I published a paper "Search Engines and Privacy" (<http://www.franken.de/users/tentacle/papers/search-privacy.txt>).

It is a plain text ASCII file with some HTML tags included as examples. Some days later a friend of mine complained that something

was wrong with the paper, he told me I had mentioned redirects where

the quoted examples did not show any redirects at all.

An HTML example which should have read

```
<a href="/r?r=http://www.test.com";>
```

was served to him as a link pointing to <http://www.test.com>.

After some testing it became obvious that this was due to his filtering

proxy, WebWasher Version 3.0 for Windows. One of the features of this proxy

is changing redirected links (which e.g. AltaVista uses) to direct

links. In this case this made the quote invalid, of course.

This is expected behavior for a HTML file, but this is a plaintext file. It

was found that the link rewriting goes along with WebWasher changing the

content type from "text/plain" to "text/html". This causes an additional

effect: the browser interprets the HTML tags contained within the textfile instead of displaying them.

So far it seems that the content type is changed if the first line of the served document is shorter than three characters (my paper started with two empty lines). In this case the first line gets dropped.

Both tested Windows versions (2.21 and 3.0) show this problem.

The code maintainers were notified.

Credits go to Jens Krabbenhoeft <jens.krabbenhoeft@fh-furtwangen.de>.

The RISKS: While filtering proxies generally are of great benefit to privacy concerned users they may (caused by bugs) do more than you expect them to do. In this case: content rewriting regardless of host or content type and changing the content type of seemingly harmless textfiles to HTML (which makes browsers interpret them).

Besides, this is a nice example for obscure bugs not showing up during regular testing. "We never experienced any bugs" does not mean that there are none.

---

## Power safety

"Marcus L. Rowland" <mrowland@ffutures.demon.co.uk>

*Mon, 23 Apr 2001 21:42:52 +0100*

I work in a suite of school science labs, most of which were

built with special "safe" mains electricity power supplies. This basically consists of a transformer unit which (a) cuts the power if a safety button is pressed, (b) splits the normal British 220-230v down to 110-115v either side of true neutral, and (c) trips if there is earth leakage of more than 5 milliamps, well below the minimum believed dangerous. Each transformer unit is a bulky box, costs about 500 UK pounds, and has to be sited in a special locked cupboard in a corridor for safety reasons.

The snag here is that all of the sockets in these labs are on these units, which has had several undesirable results:

About half of our older portable power packs and several other appliances proved to have pilot lights working on the (supposed) low voltage from neutral to earth. Mostly they tripped the breakers as soon as they were plugged in - in one case the earth connection was faulty, so the casing was suddenly live at about 100 volts. Mostly this was obvious from day one, so it was a short-lived problem. Which cost about 500 pounds to put right...

At least twice electricians working in the labs have wasted unnecessary hours on the assumption that if the "neutral" line is really 110v there is something wrong with the system.

Every couple of weeks one or another of the breakers trips (usually because someone has plugged something in with a dirty plug - grease on the plug body can conduct enough power to trip the breakers). No

immediate problem if no other equipment is in use; unfortunately all of the labs now have computers, network hubs, printers etc., there are also two incubators and a freezer which are supposed to be on all the time.

The last time this happened was in the Easter holiday, in the lab with the freezer; it contained frozen zoological specimens, and the result after several days was unpleasant, to say the least.

Whenever the power goes back on after one of these interruptions all of the computers reboot or come on if they were off. The extraction pressure safety alarms in the fume cupboards also trip, and have to be turned off manually. On several occasions equipment that was on when the power tripped has been left plugged in and switched on, and forgotten since it looked like it was off; in one case this meant that an electric heating mantle was left under a flask of oil, with nobody monitoring its temperature, for several hours after power was restored.

The cupboards containing the transformer units have ventilation slots.

Whenever I have to reset one I usually find that someone has dropped some waste paper through the slots, a fire risk.

A couple of years ago we rebuilt two labs and were able to replace two of these units with normal earth leakage and circuit breakers; there has since been no trouble, nobody has been electrocuted, and we have never had any loss of power in those labs. I'm now trying to get the rest replaced.

Every electrician I've talked to has told me that the degree of "safety" offered by these units is way beyond anything that would normally be considered necessary. The risks should be reasonably obvious; over-specified and over-sensitive safety equipment can sometimes cause hazards of its own.

Marcus L. Rowland

---

## ✈ First Workshop on Information Security System Rating and Ranking

Jack Holleran <Holleran@severnapark.com>

*Tue, 27 Mar 2001 11:43:32 -0500*

Call for Participation

FIRST WORKSHOP ON INFORMATION SECURITY SYSTEM RATING AND RANKING  
(commonly but improperly known as "Security Metrics")

Williamsburg, Virginia, 21-23 May 2001

Sponsored by:

Applied Computer Security Associates (ACSA) and The MITRE Corporation

After more than 20 years of effort in "security metrics," the evolution of product evaluation criteria identification, Information Assurance (IA) quantification, and risk assessment/analysis methodology development, has led to the widespread need for a single number or digraph rating of the "security goodness" of a component or system.

Computer science has steadily frustrated this need--it has neither provided

generally accepted, reliable measures for rating IT security nor has it applied any measures for security assurance. The goals of this workshop are to recap the current thinking on "IA metrics" activities and to formulate a path for future work on IA rating/ranking systems. Topics will include identifying workable successes or capturing lessons learned from our failures, clarifying what is measurable, and the addressing the impact of related technology insertion. The expected workshop result is the determination of "good" indicators of the IA posture of a system. The workshop will serve as a forum for group discussion, with topics determined by the participants.

Submission of a 4-to-5-page position paper is required for workshop attendance. Deadline for submission of papers EXTENDED TO 4 MAY 2001.

For further information, please see: [www.acsac.org/measurement](http://www.acsac.org/measurement)



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 21: Issue 37**

**Thursday 3 May 2001**

## Contents

- [Microsoft Is Set to Be Top Foe of Free Code](#)  
[David Farber](#)
- [DMCA: It's Like ... an Analogy Fest!](#)  
[Monty Solomon](#)
- [Recording industry threatens researcher with lawsuit](#)  
[NewsScan](#)
- [Hack attacks from China?](#)  
[NewsScan](#)
- [Space Station software problems predicted four years ago](#)  
[Philip Gross](#)
- [Incompatibility shuts down Xerox corporate network](#)  
[Nelson H. F. Beebe](#)
- [Destia shuts down service](#)  
[Doneel Edelson](#)
- [Mobile phones to prevent car theft?](#)  
[Yerry Felix](#)
- [CNN censors profane Webby nominee](#)  
[Jim Griffith](#)
- [Another problem with the DNS](#)  
[Bob Frankston](#)
- [MS security updates infected with virus](#)  
[Dave Stringer-Calvert](#)
- [Microsoft error message](#)  
[Jean-Jacques Quisquater](#)
- [Using calendar reminder service to remember anniversary of sad event](#)  
[Elinsky](#)
- [Risks of Net-connected appliances](#)  
[Robert J. Woodhead](#)
- [Re: MSN "upgrade" creates long distance calling](#)  
[Steve Holzworth](#)
- [The follow-on to James Bamford's \\*Puzzle Palace\\*](#)  
[David Farber](#)

• [Definitions for Hardware and Software Safety Engineers](#)

[Meine van der Meulen](#)

• [Info on RISKS \(comp.risks\)](#)

---

## ⚡ Microsoft Is Set to Be Top Foe of Free Code

David Farber <dave@farber.net>

Thu, 03 May 2001 09:43:23 -0400

John Markoff in *\*The New York Times\**, 3 May 2001:

Microsoft is preparing a broad campaign countering the movement to give away and share software code, arguing that it potentially undermines the intellectual property of countries and companies. At the same time, the company is acknowledging that it is feeling pressure from the freely shared alternatives to its commercial software.

<http://www.nytimes.com/2001/05/03/technology/03SOFT.html>

[Dave's IP archives are at

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

PGN]

---

## ⚡ DMCA: It's Like ... an Analogy Fest!

Monty Solomon <monty@roscom.com>

Wed, 02 May 2001 10:53:14 -0700

MEDIA GROK, 2 May 2001

We know, we know: Media coverage of the Digital Millennium Copyright Act makes your eyes glaze over. Think that's bad? Imagine the DMCA being discussed in a courtroom. This happened yesterday when a New York appeals court became ground zero for testimony on whether DVD code-busting software violates the DMCA. Reporters tried mightily - and several succeeded - to make sense of lawyers' attempts to out-argue each other.

Call yesterday's event a different kind of Hollywood strike. When the e-zine 2600.com posted DeCSS, a computer program capable of cracking DVDs' security code, a coalition of film studios struck back with a lawsuit. The studios won, and the lower court based its ruling on the DMCA-based ban on code-busting devices. 2600 appealed, its lawyers arguing that DeCSS has fair and allowable uses.

Is law so complex that it has to be fed to us in analogies? We grew dizzy trying to follow the analogy free-for-all that gripped the appeal hearing and its coverage. Let's start with the DMCA. It's like Congress deciding that the blueprint for a copying machine can't be published because it might

be used to violate the copyright laws, said Kathleen Sullivan, Stanford Law School dean. Here's one about DeCSS: It should be banned because it's akin to software that shuts off smoke detectors or airplanes' navigational systems, said DMCA defender and assistant U.S. attorney Daniel Alter, according to the New York Law Journal. The First Amendment wouldn't bar the government from prohibiting distribution of that kind of software, Alter said, and the same goes for DeCSS. No, no, no. DeCSS is "a useful tool for scientific study and journalistic inquiry - or a burglar's crowbar designed for breaking, entering and stealing," the Law Journal chimed in.

Lawyers, of course, love this kind of talk, which is no doubt why, as Inside reported, the three-judge panel was revved up enough by the legal banter to allow the session to run an extra 30 minutes. Inside ran a solid and readable analysis of the ideas that were raised, as did ZDNet, which included the tidbit that one "hacker-type" wore a T-shirt displaying the illegal DeCSS code.

But both Inside and Wired News predicted the appeals court would probably uphold the lower court's ruling. Sometimes pushing new ideas is like an uphill battle. - Deborah Asbrand

Second Circuit Weighs DVD Copying

<http://www.law.com/cgi-bin/gx.cgi/AppLogic+FTContentServer?pagename=law/View&c=Article&cid=ZZZ9P7GD8MC&live=true&cst=1&pc=5&pa=0&s=News&ExpIgnore=true&showsummary=0>

In Lively Oral Arguments, Lawyers Put Digital Copyright Act on Trial

[http://www.inside.com/jcs/Story?article\\_id=29820&pod\\_id=13](http://www.inside.com/jcs/Story?article_id=29820&pod_id=13)

Throwing the Book at DeCSS

<http://www.zdnet.com/zdnn/stories/news/0,4586,5082131,00.html>

DVD Piracy Judges Resolute

<http://www.wired.com/news/digiwood/0,1412,43470,00.html>

Court Hears Appeal of Hacker Wanting to Post Descrambling Code on Internet

<http://interactive.wsj.com/articles/SB988759509262167525.htm>

(Paid subscription required.)

Judges Weigh Copyright Suit on Unlocking DVD Shield

<http://www.nytimes.com/2001/05/02/technology/02CODE.html>

(Registration required.)

---

## **Recording industry threatens researcher with lawsuit**

"NewsScan" <newsscan@newsscan.com>

*Tue, 24 Apr 2001 09:20:08 -0700*

The litigation department of the Recording Industry Association of America (RIAA) has threatened legal action against a Princeton University computer scientist if he and his colleagues give a conference presentation this week explaining how to get around a system developed by the industry to protect

copyrighted music. The researcher, Dr. Edward W. Felton, works in the field of steganography, which develops techniques such as digital watermarking. The head of RIAA's litigation department insists: "There is a line that can get crossed, and if you go further than academic pursuit needs to go, you've crossed the line and it's bad for our entire community, not just for artists and content holders, it's everyone who loves art, and it's also bad for the scientific community." [\*The New York Times\*, 24 Apr 2001; NewsScan Daily, 24 April 2001 <http://www.nytimes.com/2001/04/24/technology/24MUSI.html>]

---

## ✈ Hack attacks from China?

"NewsScan" <newsscan@newsscan.com>  
*Mon, 30 Apr 2001 08:52:04 -0700*

The FBI cybercrime division called the National Infrastructure Protection Center is warning that Chinese hackers have publicly discussed increasing their activities in the first week of May, in celebration of two Chinese holidays and in memory of the two-year anniversary of the U.S. accidental bombing of the Chinese embassy in Belgrade. The Internet security company Vigilinx warns that it has the potential to escalate into something very damaging if emotions run unchecked. There is no evidence that attacks have been approved by the Chinese government. (AP/\*USA Today\*, 27 Apr 2001) <http://www.usatoday.com/life/cyber/tech/2001-04-27-chinese-hack.htm>

NewsScan Daily, 30 April 2001

---

## ✈ Space Station software problems predicted four years ago

"Philip Gross" <png3@cs.columbia.edu>  
*Sat, 28 Apr 2001 15:20:16 -0400*

I contributed an article to RISKS on December 8, 1997, ([RISKS-19.49](#)) about the enormous risks involved with the software of the International Space Station. 3.5 million lines of code, coming from multiple countries, with little indication of the verification methodologies. In the two subsequent issues [RISKS-19.50](#) and 19.51, anonymous posters with connections to the program agreed with and amplified these concerns.

Now we see that, indeed, difficult-to-diagnose software problems are starting to plague the craft.

"Computer problems have kept the Endeavour at the station longer than expected as astronauts try to carry out operations of a critical robot arm. The ISS has suffered a series of glitches since Tuesday that left ground controllers with only tentative command," says CNN.

(<http://www.cnn.com/2001/TECH/space/04/28/shuttle.launch.02/index.html>)

The RISKS here involve the well-known dangers of leaving debugging until the system is already in use. Although critical safety and control mechanisms

may be compromised until the problems are fixed,  
"Russian space officials refused to delay Saturday's launch but agreed to put the Soyuz in a holding pattern if the shuttle was still at the space station on Monday. Russia said it had been unwilling to postpone the Soyuz mission because the cosmonauts must replace the space station's escape craft, whose service lifetime expires at the end of the month."

The world's first space tourist may have an interesting ride...

---

## ✂ Incompatibility shuts down Xerox corporate network

"Nelson H. F. Beebe" <beebe@math.utah.edu>

*Mon, 23 Apr 2001 14:02:12 -0600 (MDT)*

\*Computerworld\* (16-Apr-2001, p. 6 and 78) has two articles on how an incompatibility between a beta release of Microsoft Windows XP and Cisco 5000 routers shut Xerox's corporate network down several times. According to the page-long column on p. 78, ``It got so bad that Xerox warned all 50,000 of its U.S. employees not to install XP betas without permission or they'd face disciplinary action.''.  
''.

Nelson H. F. Beebe, Center for Scientific Computing, University of Utah  
Department of Mathematics, Salt Lake City, UT 84112-0090 +1 801 581 5254

---

## ✂ Destia shuts down service

"Edelson, Doneel [euler:aci]" <doneel.edelson@eulergroup.com>

*Thu, 3 May 2001 17:47:14 -0400*

Destia (known as EconoPhone), a part of Viatel, shut down service to all customers Monday night or Tuesday. Thousands of people with direct-dial service (1+) are scrambling to get an alternate long-distance provider. Until then, they cannot make any long-distance calls except to 800 numbers. Also inbound 800 number service and calling cards provided by this company do not work.

---

## ✂ Mobile phones to prevent car theft?

Yerry Felix <li@esperi.demon.co.uk>

*27 Apr 2001 23:59:44 +0100*

Econet Wireless brand manager David Dzumbira said in the unfortunate event

of the vehicle being violated or vandalised, Cellstop will alert the owner by calling on his/her cellphone within seconds of the incident happening. Cellstop will dial the number three times and if these calls are unanswered or responded to, the Cellstop unit will automatically starve fuel to the engine, making it impossible to drive the vehicle, said Dzumbira.

But what if the owner forgets the phone, loses it or the phone is stolen? Or, if the phone runs out of power? And what happens if the device springs into action whilst the car is being driven by the legitimate owner?

Note that the vehicle is stopped regardless of whether the phone is ignored or answered!

Moreover, given the amount of false car alarms that seem to occur, this could be very annoying, although, being the victim of nightly car alarms in my street, I don't have much sympathy here :-)

The full article:

<http://www.mweb.co.zw/zimin/index.php?id=3176&pubdate=2001-04-27>

---

## ⚡ CNN censors profane Webby nominee

Jim Griffith <griffith@olagrande.net>

*Thu, 26 Apr 2001 20:17:34 -0500*

An interesting aspect of this year's Webby's nominees is the nomination of [www.f\\*\\*kedcompany.com](http://www.f**kedcompany.com) in the Humor category (for which I was a nominating judge). When reading the CNN article about the nominations, at

<http://www.cnn.com/2001/TECH/internet/04/26/webby.awards.reut/index.html#12>

I was interested to find that the above-mentioned site was apparently deliberately excluded from the list of nominees, probably for the profane name. The \*San Jose Mercury News\* site reported the complete list, however.

[comp.risks censors "CNN censors profane Webby nominee" as well. PGN]

---

## ⚡ Another problem with the DNS

"Bob Frankston" <rmf2gOther@bobf.Frankston.com>

*Mon, 30 Apr 2001 15:16:55 -0400*

I e-mailed a URL, <http://www.washtech.com/news/media/9387-1.html>. The spelling corrector apparently chanted washtech to washes which is a porno site! The risk here isn't so much spelling correction as the current attempt to use the DNS as a directory. The density of the namespace is just one of the many problems.

Bob Frankston <http://www.Frankston.com>

---

## ⚡ MS security updates infected with virus

Dave Stringer-Calvert <dave\_sc@csl.sri.com>  
*Sun, 29 Apr 2001 19:18:28 -0700*

Microsoft security fixes infected with FunLove virus

A virus infection of security fix files on Microsoft's partner and premier support Web sites has forced the software giant to suspend certain downloads for more than a fortnight. Microsoft issued an alert on Monday, which states that various Hotfix files on its Premier Support and Microsoft Gold Certified Partners Web sites are infected with the FunLove virus. A copy of the notice said Microsoft has stopped access "in order to protect customers" to an unspecified number of files, and expects to be able to restore access later today. Customers were advised to contact their technical account manager in the interim.

[<http://www.theregister.co.uk/content/8/18516.html>]

[Also noted by Jeremy Epstein. PGN]

---

## ⚡ Microsoft error message

Quisquater <jjq@dice.ucl.ac.be>  
*Mon, 30 Apr 2001 22:11:37 +0200*

Q276304 - Error Message: Your Password Must Be at Least 18770 Characters and Cannot Repeat Any of Your Previous 30689 Passwords

New level of security at Microsoft. Jean-Jacques Quisquater,

[The password must be Macrohard? PGN]

---

## ⚡ Using calendar reminder service to remember anniversary of sad event

<Elinsky@aol.com>  
*Tue, 24 Apr 2001 16:46:05 EDT*

This is from the "Metropolitan Diary" section of \*The New York Times\*, 23 Apr 2001. The writer unknowingly set herself up for an eerie reminder mail, by not entering the event as "Anniversary of Grandpa's death". Even if she had, the mail probably would've still contained the (presumably

inappropriate) gift suggestions.

Harriet Inselbuch signed up for a calendar reminder service on the Internet and duly entered important dates like birthdays and anniversaries. The service notifies her by e-mail a few days before an important event. One anniversary she listed was of a family death, a reminder to her to light a candle. A few days before that particular date, she did receive a message and it provided somewhat of a shock. It read, "Reminder: Grandpa's death is just around the corner" followed by three or four gift suggestions for the occasion.

---

## ✦ Risks of Net-connected appliances

"Robert J. Woodhead (AnimEigo)" <trebor@animeigo.com>  
*Mon, 23 Apr 2001 17:12:45 -0400*

After watching a breathless CNN report about Internet-enabled espresso machines, it occurs to me that one of the greatest risks of having appliances connected to the Internet is that one's refrigerator might start forwarding spam instead of simply storing it.

Robert Woodhead, Webslave & Mad Overlord <http://selfpromotion.com/>

---

## ✦ Re: MSN "upgrade" creates long distance calling ([RISKS-21.32](#))

Steve Holzworth <sch@unx.sas.com>  
*Fri, 27 Apr 2001 14:17:46 -0400*

WRAL-TV Online reports that the Microsoft Network (MSN) has agreed to pay back dozens of people who received huge Internet phone bills by mistake.

<http://www.wral-tv.com/features/5onyourside/2001/0426-msn-second-folo/>

"Combined, complainants were billed more than \$13,000 in unexpected charges.

For about a month when the Wake County customers accessed the Internet, they were routed to a long distance Chapel Hill number -- a number they did not know they had been switched to.

John Bason, a spokesman for the North Carolina Department of Justice, says the situation definitely needs to be addressed." ... "Microsoft is telling the Attorney General's office that the error was theirs and agreed to pay back consumers. Any MSN customers who were erroneously billed must file a complaint with the Attorney General's office at 919-xxx-xxxx."

Steve Holzworth, Senior Systems Developer, SAS Institute, Cary, N.C.  
Open Systems R&D VMS/MAC/UNIX <sch@unx.sas.com>

---

## ✂ IP: The follow-on to James Bamford's \*Puzzle Palace\*

David Farber <dave@farber.net>  
Wed, 25 Apr 2001 15:04:56 -0400

James Bamford  
Body of Secrets: Anatomy of the Ultra-Secret National Security Agency:  
From the Cold War Through the Dawn of a New Century

[Good review in \*The New York Times\* Sunday Book Review section,  
29 April 2001. PGN]

---

## ✂ Definitions for Hardware and Software Safety Engineers

Meine van der Meulen <M.van.der.Meulen@simtech.nl>  
Thu, 3 May 2001 09:50:50 +0200

I would like to bring the book 'Definitions for Hardware and Software Safety Engineers' under your attention. It quotes definitions in the field of hard-and software dependability engineering from over a hundred sources. When more definitions exist it quotes these to enable comparison. Much attention has been paid to cross-referencing.

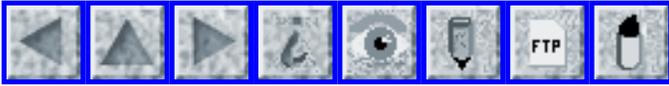
M.J.P. van der Meulen, Definitions for Hardware and Software Safety Engineers, ISBN 1-85233-175-5, Springer, London, hardcover, 342 pages.

URL: [http://www.springer.de/cgi-bin/search\\_book.pl?isbn=1-85233-175-5](http://www.springer.de/cgi-bin/search_book.pl?isbn=1-85233-175-5)

Meine van der Meulen, Max Euwelaan 60, 3062 MA Rotterdam Tel 010-4535959  
SIMTECH Engineering: [www.simtech.nl](http://www.simtech.nl) <m.van.der.meulen@simtech.nl>



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 21: Issue 38**

**Wednesday 9 May 2001**

## Contents

- [Partial Causal Analysis of the December 2000 Osprey Accident](#)  
[Peter B. Ladkin](#)
- [Lucent workers charged with selling secrets to Chinese](#)  
[NewsScan](#)
- [Citibank's meaningless privacy notice](#)  
[Vassilis Prevelakis](#)
- [Fox... hen house...](#)  
[Hendrik](#)
- [Bluetooth risks airline safety?](#)  
[Tom Worthington](#)
- [Info on RISKS \(comp.risks\)](#)

---

## ✉ Partial Causal Analysis of the December 2000 Osprey Accident

"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>  
Mon, 07 May 2001 17:22:56 +0200

Acknowledgement

Credit for the following line of reasoning is due in large part to the New Scientist reporter Duncan Graham-Rowe. The formulation here is

(obviously)  
mine.

## Disclaimer

The interpretation and reasoning presented here is based entirely on the publicly-available JAG briefing and Blue Ribbon Panel report documents, which I shall refer to as JAGB and BRPR respectively. Although written to be readable by non-specialists, it employs methods to be found in formal failure analysis techniques such as WBA. There may be errors in the reasoning and analysis, although I am reasonably confident that all such errors are minor. Please bring any errors you remark to my immediate attention (email usually suffices). The focus of this note is causal analysis and I have nothing to say here about social phenomena such as blame or responsibility.

## The Sequence of Events

First, a brief review of what the JAG determined happened in the December crash. A hydraulic line ruptured in the left nacelle. This line was part of the primary flight control system hydraulics and activates the swashplate actuators. There are three such systems, in a partially redundant configuration. At the rupture point, the line was common to Systems 1 and 3; System 1 was fully disabled, System 3 was isolated in the left nacelle, but continued to function in the right nacelle, System 2 worked left and right.

This event caused the nacelle transition to stop, and the PFCS reset button to illuminate in the cockpit. The aircrew pressed the reset button, as per procedure. The PFCS computer software then caused "rapid" pitch and thrust changes to be commanded and actuated. The rotors responded differentially in time, because the physical actuation authority in each nacelle was

different: the right nacelle had two working hydraulic systems, and the left nacelle only one. The aircrew pressed the reset button "as many as eight to 10 times [sic]" (JAGB) during the last 20 seconds of flight. The response asymmetry and resulting flight behavior of the aircraft was directly responsible for loss of control (LOC) of the aircraft and the aircraft impacted the ground in a LOC condition.

Proposed Failure Analysis based on JAGB

JAGB says: "The published procedure for responding to [a hydraulic system failure as multiply indicated in the cockpit] is to press the primary flight control system reset button. When the primary flight control reset button was pressed, a software anomaly caused significant pitch and thrust changes in both prop rotors. Because of the dual hydraulic failure on the left side, the prop rotors were unable to respond at the same rate. This resulted in uncommanded aircraft pitch, roll and yaw motions, which eventually stalled the aircraft.

During the last 20 seconds of the flight, the primary flight control reset logic was energized as many as eight to 10 times. This, coupled with the dual hydraulic failure, caused large prop rotor changes. These changes resulted in decreased airspeed and altitude and a left yaw. The crew pressed the reset button in their attempt to reset the system and maintain control during the emergency."

This clearly says

- (\*) that the PFCS software caused the PFCS to command "significant pitch and thrust changes" and that this software behavior was anomalous;
- (\*\*) that recycling the reset button "eight to 10 times" was a causal factor (in the WBA sense) of "large prop rotor changes", which were in turn a causal factor (we might wish to infer: the sole

causal factor) in the LOC.

What kind of "software anomaly" can this have been? There are, according to a common taxonomy of complex system failures, only a few possibilities. (I shall use the term "rotor excursion" for a one-time pitch and thrust change of the sort being talked about here, whatever that may consist in.)

1. A bug: the code did not fulfill the design specification; or
2. The software functioned as designed, but the design was incompatible with the overall PFCS control requirements (which implied for this situation that the PFCS should not command a rotor excursion); or
3. The software functioned as designed, and the design was compatible with the overall PFCS control requirements (that is, the PFCS requirements allowed or even implied that a rotor excursion should take place in this situation), but rotor excursions in this situation were not "expected" nor required by
  - (a) the aircraft designers;
  - (b) OPS manual;
  - (c) crew; or
4. That although a rotor excursion may have been anticipated by designers, that the effects of multiple cycling of reset, namely, multiple rotor excursions, were not anticipated by
  - (a) aircraft engineers;
  - (b) OPS manual;
  - (c) crew.

I shall say "software bug" for case 1, "software design error" for case 2, "requirements failure" for cases 3 and 4. I concluded in my [Risks-21.33](#) note

that the JAG had unequivocally indicated a software bug or a software design error had occurred. I will give my precise reasoning forthwith and I believe that reasoning is correct. However, after consulting and analysing BRPR, I see reason now to doubt the truth of the conclusion.

JAGB Quotes

In the light of these possibilities, following comments from JAGB are relevant. The briefer is Maj. Gen. Berndt, assisted by Lt. Col. Wainwright on aircraft technical matters. If unascrbed, the quotes are from Maj. Gen. Berndt.

- A. "an anomaly in the control logic in the computer software control laws which caused rapid and significant changes to prop rotor pitch each time the primary flight control system reset logic was energized."
- B. "This anomaly rendered procedures outlined in the [...] NATOPS flight manual ineffective."
- C. "This mishap was not the result of human factors."
- D. [in response to a query: "what does "anomaly" mean exactly?"] "An anomaly [here] means that something happened that was not supposed to happen, and whether that's a fault of design or structure or composition, manufacture or installation, [Maj. Gen, Berndt] do[es] not know."
- E. [Lt. Col. Wainwright] "The question was what should have happened when the PFCS button was reset with the dual hydraulic failure. The short answer is absolutely nothing."
- F. "The recommendation has been to address the anomaly within the system that caused the aircraft to accelerate and decelerate with rapid pitch changes over a short period of time."
- G. [Wainwright] "The [reset] button is multipurpose. In this particular case, it should have done nothing. [...] Because of the logic, it lights up. But when you press it, other than putting the light out, it shouldn't have really done anything at all."

Interpreting the Quotes: Reasoning to bug or software design error

Quote A clearly says that the anomaly in software-implemented control logic in software caused rotor excursions. It also says that these excursions happened upon each reset. Quote D says that something happened because of the software-implemented control logic that was not supposed to happen. One of these has the form "A caused B", the other "something with property

P

happened because of A". We may presume that the rotor excursions were the sole relevant causal consequence of the anomaly; I conclude that the rotor excursions happened and were not supposed to. It does not yet tell us what requirement is referred to by "not supposed to". It gives us a choice between 1, 2, and 3(a), but does not distinguish between them.

Quote B entails that one of 3(b) or 4(b) was the case.

Quote C appears to be inconsistent with the other information. (\*\*) implies that recycling the button appears to be a causal factor in LOC. Now, either the pilots recycled the button because (i) it was NATOPS manual procedure to do so, or because (ii) it was their choice to do so. Either (i) or (ii), whichever is the case, is a causal factor in recycling the button, which itself is a causal ancestor of the LOC. But both (i) and (ii) fall within the domain commonly termed "human factors". Hence it appears that human factors phenomena were causal ancestors of the LOC. That is in direct contradiction to Quote C. The Marines' testimony appears to be inconsistent. (That may be because they are not speaking as precisely as I am trying to.)

Quote G lets us distinguish somewhat between our choice of 1, 2, or 3 (a). It says that pressing the button should have done "nothing", that is, it should not have caused a rotor excursion. That clearly suggests that the design was not compatible with control system requirements, and rules out 3(a). It was therefore a software bug or a software design error.

This is the conclusion contained in my [Risks-21.33](#) analysis.

Quote F puts the anomaly "in the system". Design specification is not normally considered part of the system by most engineers (although I have

argued elsewhere that this may be mistaken), so I take this quote to support  
(in the sense of giving extra credence to) the conclusion that there was a  
software bug or software design error.

### Software Reparatory Measures

It should now be clear what reparatory measures would be recommended by a  
professional software engineer on the basis of this conclusion. The control  
software can be regarded as providing a "service", a particular functionality, to the PFCS. In the case of a failure of type 1, the behavior  
did not provide the service specified in the software design. In the case of  
a failure of type 2, the software provided the function specified in the  
design, but this was not the service that the rest of the PFCS required. General prophylactic measure for these cases are:

M.1) For software bugs. Inspect software against design specs; test software against design specs; remove bugs.

M.2) For software design errors. Inspect software design against PFCS design; perform integrated PFCS bench tests; remove incompatibilities between software behavior and PFCS expected behavior

It is significant, therefore, that neither of these two standard prophylactic measures was recommended by the BRPR.

Quote from the BRPR

The BRPR section on software is short and worth quoting in full.

[begin quote]

The fly-by-wire flight control system is highly dependent on high-quality  
computer hardware and software. The logic that is the basis for the many  
flight control laws and algorithms must be consistent with the overall requirement for FO/FS. This implies that if the aircraft suffers any single

failure in the electrical, mechanical or hydraulic parts of the system, there cannot be any software logic characteristic or failure that would result in an unsafe condition. The integrated flight control system must be designed, analyzed, and tested with these facts in mind.

Boeing has the lead role in development and testing of the integrated flight control system. Their Philadelphia facility has the capability to conduct integrated hydraulics, flight loads, and software testing using the Flight Control System Integration Rig. Before the mishap, the facility had limited pilot-in-the-loop capability. During the downtime, and in response to the preliminary mishap investigation results, Boeing has upgraded the capabilities of the integrated simulation facilities and is in the process of validating a set of off-nominal and failure scenarios that had been checked only by analysis during the 1996 validation and verification of the flight software. Boeing also has begun validating all flight control system emergency procedures with pilot-in-the-loop simulation runs. In addition, the company is holding an integrated flight control system review, with participation from "graybeard" experts from within and outside the company to review the requirement and the implementation of the requirements in the design.

**Conclusion:** The North Carolina mishap identified limitations in the V-22 Program's software development and testing. The complexity of the V-22 flight control system demands a thorough risk analysis capability, including a highly integrated software/hardware/pilot-in-the-loop test capability.

**Recommendation:** Conduct an independent flight control software development audit of the V-22 program with an emphasis on integrated system safety.

**Recommendation:** Conduct a comprehensive flight control software risk

assessment prior to return to flight.

Recommendation: The V-22 Program should not return to flight until the flight procedure and flight control software test cases have been reviewed for adequacy and have been evaluated in the integrated test facilities.

[end quote]

#### Analysis of the BRPR Section on Software Reliability

There is nothing in the commentary or recommendations that implies M.1 or M.2. This is remarkable. Instead, the report emphasises integrated system safety, and integrated test facilities (in which they appear to emphasise pilot-in-the-loop testing).

Standard system-safety and risk assessment involve identification and analysis of hazards, including assessing the likelihood of a hazard condition, and identifying the likelihood that an accident will result from a specific hazard. The hydraulic failure is a specific hazard; they say from this hazard "there cannot be any software logic characteristics or failure that would result in an unsafe condition". They do not say "result in an accident", or "result in an unsafe condition or accident". This suggests that they believe that more factors were involved in the accident than the software logic alone.

From the JAGB, we concluded that there was a bug or a software design error that caused behavior that resulted, along with multiple resets and the asymmetric physical response of the rotors, in the LOC, which itself resulted in the accident. An informal WB-Graph of the accident according to the analysis of JAGB would contain the following chains of causal factors. (To obtain a partial graph from these chains, superimpose identically labelled features, e.g., "PFCS behavior" in the first three chains. I emphasise: the WB-Graph will be partial.)

- C1) HF -> multiple resets -> PFCS behavior -> dynamic behavior of AC -> -> LOC -> Accident
- C2) Physics of AC design and configuration -> dynamic behavior of AC
- C3) PFCS intentional design -> PFCS behavior
- C4) PFC anomalies -> PFCS behavior
- C5) Software subsystem design anomalies or bugs -> PFC anomalies

Prophylactic measures are supposed to break the causal chains somewhere.

Integrated testing including pilot-in-the-loop enables C1 to be broken by

modifying the human behavior that led to the multiple resets, by changing or

modifying procedures. C2 cannot be broken, because it is physically necessary, although the specific behavior can thereby be changed. No recommendation is made here to do this. Likewise C3 cannot be broken, because it represents physical necessity: PFCS design will causally result

in behavior of the PFCS whenever the PFCS is activated (although of course

it will not if the PFCS is never activated). PFCS design may be changed, to

result in different behavior, of course, and this is what I take to be the

purpose of risk assessment: how to mitigate the consequences of the hazard

through PFCS change. C4 may be broken by removing anomalies; similarly C5

may be broken by removing anomalies in the software subsystem.

In a thorough safety audit, all chains that could be broken would be considered. But the BRPR speaks nowhere above of breaking C4 and C5, because

nowhere is anything approaching M.1 or M.2 suggested. The BRPR concentrates

instead on C1 (integrated testing with pilot-in-the-loop) and modifications

in C3. (We may presume that modifications concerning chain C2 are all considered in another section of the report.)

Comparing with the goals of the report and the qualifications of the panel

members, this selection is comprehensible only on the hypothesis that these chains C4 and C5 aren't in fact there. But the JAG report implied that they were.

Well, are they or aren't they there? JAGB says yes, BRPR implies no.

Suppose they are not there, and that the PFCS functioned as designed and expected by its engineers. What would the accident scenario look like, consistent with the other information provided by JAGB? Considering the taxonomy 1-4, I think only three possibilities present themselves.

One possibility, suggested by Peter Neumann, is that the basic behavior with single reset was known, but the behavior with multiple resets was not considered either in the NATOPS flight manual procedure definition, or by the designers. The effects of multiple resets was not known. The resulting behavior turns out to interact badly with the asymmetric hardware response and resulted in this incident in the LOC.

The second possibility is that the behavior even of a single reset was not considered in the integrated control systems. It was known by PFCS engineers that a rotor excursion would be commanded, but the physical characteristics of that rotor excursion, especially the asymmetrical rotor response, had not been determined.

The third possibility, and I would imagine the least likely, is that the potential behavior in this situation was generally anticipated by engineers, but not known by or to the flight crew.

I believe it is known whether one of these possibilities was the case. However, it is not inferable from the public information. It is not my purpose to speculate. I shall stop here.

Peter B. Ladkin <<http://www.rvs.uni-bielefeld.de>> University of  
Bielefeld

---

## ⚡ Lucent workers charged with selling secrets to Chinese

"NewsScan" <[newsscan@newsscan.com](mailto:newsscan@newsscan.com)>  
*Fri, 04 May 2001 06:30:13 -0700*

Federal authorities arrested two Lucent scientists and a third man yesterday, charging them with stealing software associated with Lucent's PathStar Access Server and sharing it with a firm majority-owned by the Chinese government. The software is considered a "crown jewel" of the company. Chinese nationals Hai Lin and Kai Xu were regarded as "distinguished members" of Lucent's staff up until their arrests. The motivation for the theft, according to court documents, was to build a networking powerhouse akin to the "Cisco of China." The men face a maximum five years in prison and a \$250,000 fine. (\*USA Today\*, 4 May 2001 <http://www.usatoday.com/life/cyber/tech/2001-05-03-lucent-scientists-china.htm>)

NewsScan Daily, 4 May 2001, written by John Gehl and Suzanne Douglas, [editors@NewsScan.com](mailto:editors@NewsScan.com))

---

## ⚡ Citibank's meaningless privacy notice

VASSILIS PREVELAKIS <[vassilip@dsl.cis.upenn.edu](mailto:vassilip@dsl.cis.upenn.edu)>  
*Thu, 3 May 2001 02:03:04 -0400 (EDT)*

Citibank(South Dakota, N.A.) sent a leaflet to its customers to "...  
tell you  
how you can limit our disclosing personal information about you."

Observe what great choice Citibank customers have:

[...]

Categories of Nonaffiliated Third parties to whom we may disclose personal information

Nonaffiliated third parties are those not part of the family of companies controlled by Citigroup Inc.

We may disclose personal information about you to the following types of nonaffiliated third parties:

- \* Financial services providers, such as companies engaged in banking, credit cards, consumer finance, securities and insurance,
- \* Non-financial companies, such as companies engaged in direct marketing and the selling of consumer products and services

If you check box 1 on the Privacy Choices Form, we will not make those disclosures except as follows. First, we may disclose information

^^^^^^^^^^^^^^^^^^^^

about you as described above in "Categories of Personal Information we collect and may disclose" to third parties that perform marketing services on our behalf or to other financial institutions with whom we have joint marketing agreements. Second, we may disclose personal information about you to third parties as permitted by law,

^^^^^^^^^^^^^^^^^^^^

including disclosures necessary to process and service your Citi Card account.

[...]

Sharing with Citigroup Affiliates (Box 2)

The law allows us to share with our affiliates any information about

your transactions or experiences with you.

Unless otherwise permitted by law, we will not share with our

^^^^^^^^^^^^^^^^^^^^

affiliates other information that you provide to us or that we obtain from third parties (for example credit bureaus) if you check Box 2 on the Privacy Choices Form.

[...]

The options the clients are given are non-sensical as the bank retains the right to share information "as permitted by law" with just about everybody.

Let's consider Box 1. Assuming that Citibank does not break the law, if the customer does not check the box, Citibank can share personal information with third parties. If the customer checks the box, Citibank "may disclose personal information to third parties"

So whether Box 1 is checked or not the effect is the same unless Citibank breaks the law in sharing information with third parties. Only in this case checking the box makes a difference. If the box is checked, the customer essentially asks Citibank to stop performing these illegal activities.

Let us now consider box 2. Regardless of the state of the box, Citibank can share with its affiliates "any information about [Citibank's] transactions or experiences with [the customer]."

The information that box 2 is supposed to control is information "obtain[ed] from third parties". Again if the box is not checked then this information may also be shared, while if the box is checked personal information may still be shared unless prohibited by law.

Great choice!

On their web site "<http://www.citibank.com/privacy>"; Citibank claims:  
"6. We will tell customers in plain language initially, and at least once annually, how they may remove their names from marketing lists. ..."

If the language that was used in the leaflet is "plain" then Citibank must assume that all their clients are lawyers.

In fact the whole purpose of the leaflet is to \*pretend\* that Citibank cares about the privacy of the customers, while retaining the right to distribute the personal information of their customers in any way they like.

I have no problem with that - if I want privacy I can open a dollar account with a European bank and enjoy the protection of the EU laws. I \*do\* object, however, to being handed a document like that which treats me like an idiot.

Vassilis Prevelakis, University of Pennsylvania

---

## ⚡ Fox... hen house...

Hendrik <subsc15@hiz.bc.ca>

Tue, 8 May 2001 19:55:20 +0900

Microsoft strikes banking deal [Excerpt from AP Internet news service]

Microsoft Corp. on Monday announced a deal to provide banks with software

designed to make their Internet transactions ultra-secure. The technology, which works in the Windows 2000 operating system, is designed

to allow banks to be sure of whom they're dealing with on the Internet.

It matches a security framework designed by Identrus, an alliance of 150

of the world's largest banks. The deal involves Microsoft, Unisys Corp. of Blue Bell, Pa., and Ireland-based Baltimore Technologies, which

has its U.S. headquarters in Boston. Baltimore is providing its Public

Key Infrastructure security system, and Unisys is providing help using the

system. [Full article at:

<http://www.infobeat.com/fullArticle?article=406981693>]

No, there is no risk of me believing this will work. Maybe owners of Microsoft Encarta can find the suitable definition of the term "ultra-secure", when applied in the context of Windows 2000...?

---

## ✈ Bluetooth risks airline safety?

Tom Worthington <tom.worthington@tomw.net.au>

*Tue, 08 May 2001 12:43:52 +1000*

An advertisement by Toshiba in the Australian Financial Review Monday 7 May 2001 (page 10: "Portege 3490 with Bluetooth - always ready to network") suggests that Toshiba laptops can be routinely carried on aircraft switched on, with Bluetooth devices transmitting:

> "Imagine two strangers, each carrying Bluetooth-enabled Portege 3490s ...  
> In a fraction of a second the Bluetooth module within each detects the presence of the other. ... And complete strangers can start playing chess together on long flights"

Apart from being misleading as laptop computers are not designed to be left on while being carried, this appears at odds with routine airline practice requiring electronic devices to be switched off during take-off. The use of radio transmitters by passengers is usually prohibited at any time on an airline. This is discussed in the Draft Advisory Circular AC 91.22 (0), FEBRUARY 2000, "PORTABLE ELECTRONIC DEVICES" from the Australian Civil Aviation Safety Authority:

<http://www.casa.gov.au/prod/avreg/newrules/download/ac/091%5F22.pdf>

In practice, Bluetooth's very low-power spread-spectrum transmitter would be unlikely to cause interference to an aircraft's systems. However, it would

be unwise to encourage Bluetooth's use on airlines until this is accepted by airline safety authorities.

PS: It is possible to use a transmitter in some aircraft. Particularly when it is a hot air balloon over Parliment and you have a Senator assisting you: <http://www.tomw.net.au/nt/balloon.html>

PPS: More on wireless: <http://www.tomw.net.au/2001/wgw.html>

Tom Worthington FACS; Director, Tomw Communications Pty Ltd ABN: 17 088 714 309  
<http://www.tomw.net.au>; Vis.Prof AustralianNatlUniversity; Austrl. Computer Soc



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 21: Issue 39

Friday 11 May 2001

## Contents

- [U.S. Air Force blasts Outlook security patch](#)  
[Yves Bellefeuille](#)
- [Univ. Virginia prof uses computer to catch cheaters](#)  
[Richard Kaszeta](#)
- [Potential timestamp overflow on 9 Sep 2001](#)  
[Don Stokes](#)
- [Excel-lent leaks](#)  
[Christophe Augier](#)
- [Foolish wireless network access policies and spam engines](#)  
[Thor Lancelot Simon](#)
- [Cops say teen concocted radio calls](#)  
[Steve Hutto](#)
- [The RISKS spam crossover has finally taken place!](#)  
[RISKS](#)
- [DMV screws up on licenses](#)  
[PGN](#)
- [To drive or to avoid identity theft: mutually exclusive?](#)  
[Brett Glass](#)
- [Re: Recording industry threatens researcher](#)  
[Douglas W. Jones](#)

● [16th Annual Software Engineering Symposium 2001](#)

[Carol Biesecker](#)

● [Info on RISKS \(comp.risks\)](#)

---

## ✶ U.S. Air Force blasts Outlook security patch

Yves Bellefeuille <[yan@storm.ca](mailto:yan@storm.ca)>

*Fri, 04 May 2001 17:28:25 -0400*

A paper, "Reinforcing dialog-based security," by Martin Carlisle and Scott Studer, of the US Air Force Academy Computer Science Department, is to be presented on 5 Jun 2001 at the IEEE Systems, Man, and Cybernetics Information Assurance Workshop in West Point, NY, sponsored by NSA. The paper criticizes the Outlook 2000 SR-1 E-mail Security update [[RISKS-21.36](#)], developed in response to the I Love You virus to block certain types of attachments.

[Source: \*Infoworld\* Article by Sumner Lemon, PGN-ed. Thanks also to Monty

Solomon. <http://www.infoworld.com/articles/hn/xml/01/05/04/010504hnairf.xml>]

---

## ✶ U. Virginia prof uses computer to catch cheaters

Richard Kaszeta <[kaszeta@me.umn.edu](mailto:kaszeta@me.umn.edu)>

*Tue, 8 May 2001 11:01:03 -0500 (CDT)*

The latest Wired News includes an article that discusses how a University of

Virginia professor nabbed 122 students for plagiarism using a computer program he wrote himself. The program basically compares papers and looks for phrases shared between papers. Using this technique, the professor caught 122 of 500 students in his class cheating. All the students caught were referred to the schools Honor committee.

(<http://www.wired.com/news/school/0,1383,43561,00.html>)

As a seasoned systems administrator in a college department and former student myself, I know that in a college environment, the efforts to which some students will go to cheat show an astonishing amount of creativity--breaking into accounts, exploiting lack of permission control on other users' accounts, searching through the recycle bins, etc. The use of technology in this environment has made cheating easier, and harder to trace.

The risk is that some of the students are probably innocent, merely being guilty of having their own papers copied without their knowledge. Indeed, some of the students claim towards the end of the article that exactly that has happened.

Unfortunately, the technology of online composition and submission of papers (as typically done at most Universities) lacks sufficient security, encryption, and authentication standards.

Richard W Kaszeta, Engineer, University of MN, ME Dept  
rich@kaszeta.org <http://www.kaszeta.org/rich>

## ⚡ Potential timestamp overflow on 9 Sep 2001

Don Stokes <don@daedalus.co.nz>  
*Mon, 07 May 2001 01:46:08 +1200*

In case no-one else has noticed ...

On 9 Sep 2001, at 1:46:40 UTC, the Unix `time_t` value (the number of seconds since the 1st of January 1970 0:0:0 UTC) ticks over from 999999999 to 1000000000, thereby moving from being a nine digit decimal number (as it has been since 1973) to a ten-digit number.

Anyone storing decimal `time_t` values into a nine-digit field is going to have an interesting problem on that date.

---

## ⚡ Excel-lent leaks

"Christophe Augier" <augier@altran.com>  
*Fri, 4 May 2001 09:14:05 -0400*

This amusing story was told to me by a friend, whose company name will stay hidden. Once upon a time, there was a sales director in a big spirit and wines company. This person managed the whole team for a big European country. One day she had to take the decision of laying off a high position salesman, working for this company since years. Because of the turmoil generated inside the team by this firing, she wanted to set the organization

changes, and she made a new Org-chart and asked her administrative assistant to forward the file to all the sales team.

Well... Everything looks fine, since you don't know yet that the new org-chart was made on an Excel Book. "Book" means several sheets... So, what was distributed to the whole team?....

Sheet 1 : The Org-chart : ok. At least THAT was good.  
Sheet 2 : All the names of the salesman for the whole country, their salary, and appreciation commentaries (kind off:"this guy will never succeed / he is a burden") and raises projection. By the way, with a good raise projection for herself :)  
Sheet 3 : A road-map to lay off the old salesman. all the information, dates, argumentation needed to get rid of him.

Isn't that nice?

Conclusion : A nightmare ! all the guys with a bad appreciation went postal (one guy from the south realized that his "sibling" of the north was making double money for the same work & results, etc...). I guess they should have had a lot of resignation... And a friend of the fired salesman forwarded the mail to him, giving him good material for the lawsuit he was engaging against the company.

The risks? When you don't know how to use Excel or any software : don't use it for critical information ! When you send an e-mail : watch out what you are sending !

## **✶ Foolish wireless network access policies and spam engines**

Thor Lancelot Simon <tls@panix.com>

3 May 2001 20:53:30 -0400

A local university has deployed a large 802.11 wireless network without WEP or any other security measure. Given the complexity of distributing WEP keys to huge numbers of students, faculty, and staff, not to mention the need for periodic changes, and the notorious insecurity of WEP itself, this might seem to be a reasonable choice. They have decided to provide public access to their IP connectivity for those within radio range of their campus rather than tackle the very significant issues associated with restricting access.

The RISK? Their campus mail-handling machines will relay mail to any inside or outside destination if it's received from an address "inside" their campus network. The network architecture they've chosen for their wireless deployment dictates that anyone can walk onto their (large, urban) campus, or even just park his car outside, and spam away freely with hundreds of megabits per second of bandwidth to most points on the Internet.

Basically, their entire campus just became a "safe harbor" for anyone owning a laptop and wireless card to do nefarious things to outside hosts with, essentially, perfect, impenetrable anonymity. There's not even a billing record for a throwaway dialup account to trace back; just a MAC

address that  
can be trivially changed and the knowledge that it was used  
\*somewhere\* on  
their campus to do Bad Things at some point in the past.

Thor Lancelot Simon <tls@rek.tjls.com>

---

## **✶ Cops say teen concocted radio calls**

Steve Hutto <shutto@kata.chezns.org>

*Fri, 11 May 2001 12:07:04 -0600 (MDT)*

\*Rocky Mountain News\*, 11 May 2001 (excerpt)

[http://rockymountainnews.com/drmn/local/article/0,1299,  
DRMN\\_15\\_455095,00.html](http://rockymountainnews.com/drmn/local/article/0,1299,DRMN_15_455095,00.html)

"A 16-year-old boy using a handheld radio and a computer  
allegedly sent Denver  
police cruisers and a helicopter to fake emergencies and called  
officers off  
legitimate 911 calls for more than a month before getting caught.

Police said Thursday that the teen managed to hack into the  
department's  
computer-controlled radio system, program his radio to transmit  
on the  
department's frequency from his Southwest Denver home and then  
took on the  
alias of Jerry Martinez, a fictitious Denver police officer."

The teen enjoyed chatting with police helicopters flying  
overhead as well as  
reporting non-existent emergencies and accidents.

Eventually, police dispatchers caught on. When he called  
requesting  
license-plate information, they kept him talking for an hour and  
a half while

the FCC physically located him using "special equipment". The final straw came a couple days later when an informant talked him into modifying another radio to transmit on police frequencies. The teen was charged with a dozen misdemeanors and a dozen felonies.

The best part of the story is near the end:

"Police have not determined how the teen allegedly hacked into their radio system. The police department's emergency radio system uses two sets of security identification codes and a computer to prevent unauthorized access."

Considering all the possible risks here is a scary proposition, especially if used judiciously by someone with a bit more restraint.

-Steve Hutto

---

## **✶ The RISKS spam crossover has finally taken place!**

RISKS List Owner <risiko@csl.sri.com>

*Wed, 2 May 2001 16:31:28 PDT*

Subsequent to the posting of [RISKS-21.35](#), for the very first time in our almost 16 years of RISKS issues, the number of spam e-mail messages has exceeded 50% of all RISKS e-mail (despite filtering by our incoming mail systems). This is an extremely unfortunate happening, because I first have to filter out and delete all the e-junk before I can even hope to ferret out

the good stuff that you are faithfully submitting. Also noteworthy is that the volume of legitimate contributions continues to increase (which is wonderful because more of you are responding, but is sad because I cannot include everything)...

I hate to recommend draconian anti-spam measures, but the problem is clearly out of control. We are of course opposed to short-sighted legislation and censorship -- especially if it overzealously filters out desired e-mail. Perhaps it is time to implement some radical techniques such as that described in a 1992 paper by Cynthia Dwork and Moni Naor, Pricing Via Processing Or Combatting Junkmail, Proc. Crypto 1992, LNCS 740.

PGN

---

## **DMV screws up on licenses**

"Peter G. Neumann" <Neumann@CSL.sri.com>  
*Fri, 11 May 2001 07:58:14 -0700 (PDT)*

[TNX to KFWB item from Lauren Weinstein]

### DMV Sends Licenses To Wrong Addresses

California's Department of Motor Vehicles has mailed as many as 3,000 driver's licenses to the wrong addresses due to a malfunction in an 8-year-old sorting machine that processes more than 7 million licenses and ID cards every year. DMV officials say they will retire the machine.

It is unclear exactly how many licenses were erroneously mailed. There are 202 confirmed errors so far, but officials expect more.

Officials say they are not concerned about the stray licenses. They are asking those who receive a license that does not belong to them to return it. Those who do not could face criminal charges.

For the actual license owners, the DMV will issue a new license number upon request to prevent identity theft.

Motorists with questions should call DMV's information line at 1-800-777-0133.

---

## **🔥 To drive or to avoid identity theft: mutually exclusive?**

Brett Glass <brett@lariat.org>

*Fri, 11 May 2001 09:36:11 -0600*

This February, my driver's license came up for renewal -- a fairly ordinary event. I expected to wait briefly at the local Department of Transportation office, take an eye test, have an unflattering photo taken, and be on my way in short order. Alas, it was not to be. When I submitted the renewal form, I was shocked and dismayed to discover that the clerk would not renew my license unless I placed my Social Security number on it. There was no Privacy Act notice on the form (as required by the 1974 Privacy Act), so I asked the clerk why she believed she could demand my Social

## Security

number -- and refuse me a license if I did not supply it.

What I found out was chilling. Not only does Federal Law -- thanks to the striking of a single word from a huge statute -- require that drivers submit their Social Security numbers when applying for licenses. It also requires that all of the information maintained about a driver by a state -- including that number -- be revealed to virtually all comers. Here are the details of these onerous laws, along with additional information about the laws in my particular state (which are typical of state laws throughout the country). I'll also describe the way in which one state is fighting the Federal laws that would require it to compromise its citizens' privacy and subject them to trivially easy identity theft.

## Requirement for Collection

Very recently, welfare reform legislation changed Federal law to require that states collect all citizens' Social Security numbers when they apply for driver's licenses. (Earlier versions of the law only required it if one applied for a \*commercial\* driver's license, on the theory that one could threaten a deadbeat parent's livelihood if he or she required that license to work.) But a subtle amendment, slipped in just recently, struck the word "commercial," requiring the SSN to be collected from all applicants. The ironically numbered passage at 42 USC 666(a) (see <http://www4.law.cornell.edu/uscode/42/666.html>) says:

>(13) Recording of social security numbers in certain family

matters. -

>Procedures requiring that the social security number of -

>

> (A) any applicant for a professional license, driver's  
> license, occupational license, recreational license, or  
> marriage license be recorded on the application;

>

> (B) any individual who is subject to a divorce decree,  
> support order, or paternity determination or acknowledgment  
be

> placed in the records relating to the matter; and

>

> (C) any individual who has died be placed in the records  
> relating to the death and be recorded on the death  
certificate.

> For purposes of subparagraph (A), if a State allows the use  
of a

> number other than the social security number to be used on  
the

> face of the document while the social security number is  
kept on

> file at the agency, the State shall so advise any  
applicants.

Note that while a different number may be used on the "face" of  
some

licenses, the state must still collect the Social Security  
number. Also note

that many of the items mentioned above are public records which  
can be

accessed by all comers (in some cases, due to open record laws  
such as

Wyoming's).

#### Requirement to Disseminate

The requirement that states disseminate Social Security Numbers  
it has

collected comes from a law misleadingly titled the "Drivers'  
Privacy

Protection Act." This law did in fact start out as a law to  
protect drivers'

privacy, but due to amendments promoted by monied lobbyists it

has just the opposite effect. (It is said, justifiably, that the law should really be called the "Drivers' Privacy Prevention Act.")

The law is reproduced on the Web at

<http://www.networkusa.org/fingerprint/page1b/fp-dmv-records-18-usc-123.html>

Note that this law makes ALL of the information you submit to your state's DMV/DOT available to \*anyone\* who claims that it's needed for any business purpose. If I wanted your driving records and SSN, all I'd have to do is walk into the courthouse and claim that you owed me a dollar.

The DPPA was challenged by the Alabama Attorney General on states' rights grounds and was ruled unconstitutional by a Federal district court:

<http://www.networkusa.org/fingerprint/page1b/fp-dppa-al-appeal.html>

However, the US Supreme Court, in a chilling ruling that dubbed our personal information "items in interstate commerce" and therefore subject to Congressional control under the Commerce Clause, reversed the Circuit Court:

<http://caselaw.lp.findlaw.com/cgi-bin/getcase.pl?court=US&navby=case&vol=000&invol=98-1464> [SPLIT URL]

In retrospect, challenging the law on the basis of states' rights was probably a big mistake. The Alabama AG might have had better success had he cited the right to personal privacy delineated in *Griswold v. Connecticut*.

State SSN Requirements And Public Records Acts

The laws of many states also mandate the collection of Social Security numbers -- and make the forms containing those numbers public records. I live in Wyoming, and this is the case in my state. (The details of the laws are instructive because they are similar to those in other states; however, if you're uninterested in the specifics, you may want to skip down to the heading "Michigan's Challenge" to learn more about a recent challenge to the Federal laws.)

Wyoming law, at W.S. 31-7-111 (b) ("W.S." = "Wyoming Statutes"), describes the information required on a driver's license application:

>(b) The application shall include:

>

> (i) The full legal name and current mailing and residential address of the person;

>

> (ii) A physical description of the person including sex, height and weight;

>

> (iii) Date of birth;

>

> (iv) The person's social security number or other numbers or letters deemed appropriate on applications for instruction permits, driver's licenses, commercial driver's licenses and commercial driver instruction permits;

Note that the statute does provide for an alternative; however, the phrase "deemed appropriate" (By whom? What is the standard of propriety?)

is vague. The clerk said that she, at least, deemed no other numbers or letters to be "appropriate."

The law also requires the state to keep the application on file even after it is processed. According to W.S. 31-7-120,

>31-7-120. Records to be kept by division; exception.

>

> (a) The division shall maintain a readily available file of and

> suitable indexes for:

>

> (i) All license applications denied with the reasons for denial

> noted thereon;

>

> (ii) All applications granted;

>

> (iii) Every licensee whose license has been suspended or revoked

> and the reasons

> for the action;

>

> (iv) All accident reports and abstracts of court records of convictions

> received under the laws of this state with suitable notations for

> each licensee showing the convictions of the licensee and the

> traffic

> accidents in which he has been involved.

What's more, the application is, according to the state's open records

law, a public record that anyone may access. According to W.S. 16-4-201(a)(v),

>(v) "Public records" when not otherwise specified includes the original

>and copies of any paper, correspondence, form, book, photograph, >photostat, film, microfilm, sound recording, map drawing or

other

>document, regardless of physical form or characteristics that  
have been  
>made by the state of Wyoming and any counties, municipalities  
and  
>political subdivisions thereof and by any agencies of the state,  
>counties, municipalities and political subdivisions thereof, or  
received  
>by them in connection with the transaction of public business,  
except  
>those privileged or confidential by law;

Needless to say, an open records law would be meaningless if a  
government  
agency were allowed to censor the records on its own initiative  
before  
revealing them! So, if the Social Security number were to be  
redacted,  
the Department of Transportation would have to be specifically  
authorized  
by law to do it. Alas, as in most states, there appears to be no  
Wyoming  
statute declaring the form -- or the information on it,  
including the  
Social Security number -- to be privileged or confidential.  
Worse still,  
any such declaration would arguably be overridden by the Federal  
statute.

## Wyoming Violates the Privacy Act

The Wyoming Department of Transportation (WYDOT) also violates  
the  
Federal Privacy Act by failing to place a Privacy Act Notice on  
its  
driver's license applications. 5 U.S.C. § 552a note (1982) (see  
<http://www.usdoj.gov/foia/privstat.htm>), also called the Privacy  
Act of  
1974, provides that:

>(b) Any Federal, State or local government agency which  
requests an  
>individual to disclose his social security account number shall

inform  
>that individual whether that disclosure is mandatory or  
voluntary, by what  
>statutory or other authority such number is solicited, and what  
uses will  
>be made of it.

Without a Privacy Act notice (which does \*not\* appear on the  
current  
application), WYDOT is not permitted to collect Social Security  
numbers  
whether there is a Federal requirement for it to do so or not.  
This was  
affirmed in *Gredinger v. Davis* (see  
<http://www.networkusa.org/fingerprint/page2/fp-ssn-davis.html>).  
Nonetheless, the state's Department of Transportation refuses to  
issue  
the license based on an otherwise complete application.

#### Michigan's Challenge

The Michigan Secretary of State is challenging the Federal laws  
that,  
together, require collection and disclosure of Social Security  
numbers.

The two press releases at

<http://www.sos.state.mi.us/pressrel/active/010227-1n.html>

and

<http://www.sos.state.mi.us/pressrel/active/010104-1n.html>

describe the progress of the case.

When the Federal law was modified to encompass all drivers'  
licenses, it  
was claimed by overzealous legislators that the change was  
necessary to  
collect drivers' Social Security numbers to pursue deadbeat  
parents. The  
Michigan Secretary of State, however, says that it would  
actually make

their system LESS effective, not more, because of the actual logistics of tracking deadbeat parents. In the second press release cited above, her office wrote:

>Secretary Miller argued in her exemption requests that the collection of  
>Social Security numbers would violate the strong interest her department  
>has in protecting customer privacy. The process would be expensive and  
>counterproductive to measures already in place by the state to track  
>those owing child support. It was also noted that in addition to being  
>an unfunded federal mandate, the law raises questions about its ability  
>to protect the welfare of Michigan children.

>  
>This federal law applies only to citizens with driver licenses, which  
>severely limits the ability to locate deadbeat parents. Consequently in  
>Michigan, more than four million people would be overlooked because the  
>databases containing records of suspended drivers, state identification  
>card holders and those on the Qualified Voter File would be excluded  
>from any search.

>  
>Currently, the Michigan Family Independence Agency (FIA) conducts  
>searches of all Secretary of State databases for deadbeat parents using  
>a name, or even part of a name. It is successful in obtaining  
>identification 90 percent of the time, according to figures from FIA and  
>the Secretary of State. The Secretary of State estimates that the  
>success rate would drop to about 60 percent under the federal law

>primarily because searches would be limited to only residents with  
>driver licenses. Other problems with the federal law identified by  
>Secretary Miller include:  
>  
>\* States would not be required to verify the Social Security numbers  
>collected by their Department of Motor Vehicles or Secretary of State  
>offices are correct.  
>  
>\* The law represents a significant duplication of effort because both  
>the Internal Revenue Service and Michigan Department of Treasury already  
>have databases of Social Security numbers.  
>  
>\* The law places the majority at risk for possible misuse of their  
>Social Security numbers and identity fraud in attempts to target a  
>minority guilty of delinquent child support payments.

Unfortunately, because the suit is being brought in only one Federal  
district, a ruling in favor of the Michigan Secretary of State would not  
be binding in the rest of the country.

#### My Status

Deb Ornelas, an administrator at the Wyoming Department of Transportation, insists that I submit my Social Security number in order to keep my license. She says that she believes that her hands are tied by both state and Federal law. Indeed, due to a lack of vigilance by legislators and citizens, they may well be unless the law is challenged and that challenge is successful. Thus, I may need to decide between the risk of trivially easy identity theft or loss of my right to

drive.

Suggestions regarding how to proceed, and help in starting an initiative to have the Federal laws changed, would be greatly appreciated.

--Brett Glass

---

## ⚡ Re: Recording industry threatens researcher ([RISKS-21.37](#))

"Douglas W. Jones" <jones@cs.uiowa.edu>

*Fri, 4 May 2001 11:00:07 -0500 (CDT)*

I cannot avoid suggesting an analogy (in the spirit of the analogy first cited in the previous item in the same Risks Digest):

If I present a paper about the construction of a gun, nobody threatens to sue me. In fact, if I possess a gun, I am protected by the second amendment. My right to talk about and possess guns is unlimited. Only my use of guns to injure or kill is regulated by law.

If, on the other hand, I wish to present a paper describing the weakness of a commercial encryption product, where that weakness could be used to violate a copyright law, my first amendment right to free speech is irrelevant. Discussion of the weakness itself is forbidden, without regard to whether I construct a mechanism to exploit that weakness and without regard to whether I actually injure the interests of a copyright holder.

We can conclude from this that the second ammendment is far stronger than the first ammendment, or that the interests of copyright holders are far more important than the right to life of potential shooting victims.

It is ironic that the entertainment industry is directly behind this round of attacks on the first ammendment!

Doug Jones <jones@cs.uiowa.edu>

PS: <http://www.cs.uiowa.edu/~jones/compress/#intro> contains, in the solution to machine problem 3, the source code of a program that I believe would violate the DMCA if anyone were stupid enough to use a ROTn Caesar cypher to protect a copyrighted work (distributing the work in ROTn encrypted form, and selling the value of n to to customers). This program finds n for almost any ROTn encrypted English text.

---

## **★ 16th Annual Software Engineering Symposium 2001**

Carol Biesecker <cb@sei.cmu.edu>  
*Mon, 7 May 2001 19:30:22 +0000 (UTC)*

Catalysts for Improving Acquisition and Development of  
Software-Intensive Systems

SEI 16th Annual Software Engineering Symposium 2001  
15 -- 18 Oct 2001  
Grand Hyatt at Washington Center, Washington, D.C.

For more information about the Symposium, contact

Symposium 2001 Conference Coordinator

Phone: 412 / 268-3007

FAX: 412 / 268-5556

E-mail: [symposium@sei.cmu.edu](mailto:symposium@sei.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 21: Issue 40**

**Sunday 13 May 2001**

## Contents

- [Word file turns into two disjoint texts](#)  
[Clive Page](#)
- [Check everyone's Vodafone voicemail](#)  
[Andrew Goodman-Jones](#)
- [Car 54, where are you?](#)  
[David Lesher](#)
- [Euro risks, part 1](#)  
[Paul van Keep](#)
- [Euro risks, part 2](#)  
[Paul van Keep](#)
- [Thieves R Us](#)  
[Mike Godwin via Dave Farber](#)
- [Re: Citibank's meaningless privacy notice](#)  
[Zygo Blaxell](#)
- [Re: Using calendar reminder service ...](#)  
[Nikita Borisov](#)
- [Re: MSN "upgrade" creates long distance calling](#)  
[Bob Frankston](#)
- [Risks of not monitoring field-deployed systems](#)  
[John Connor](#)

● [Re: UPS Shutdown](#)

[Diomidis Spinellis](#)

[Chris Smith](#)

● [Info on RISKS \(comp.risks\)](#)

---

## ⚡ Word file turns into two disjoint texts

Clive Page <cgp@leicester.ac.uk>

*Fri, 11 May 2001 15:25:04 +0100*

The risks involved when using Microsoft Word, which merely hides text when it appears to have been deleted, have been covered before. Today, however, I encountered an extreme example which nearly fooled me. A computer company responded to my request for a quotation for disc drives by sending me an email with the quotation as a Word attachment.

As a user of Unix and Linux systems, I find Word files mildly annoying, but I can decode most of them easily using the Unix utility `word2x`; this works quite well except on files which contain graphics. This time, however, the resulting text file revealed a quite different letter, intended for someone at the University of Strathclyde, for a completely different set of equipment. When I copied the file to a Windows box and used Word to view it, it did not show this at all, only the quotation which I had requested. So: one Word file is capable of producing two entirely disjoint texts.

The Unix "strings" utility also revealed only the Strathclyde quotation, so

it appears that the deleted text is left as ASCII, while the undeleted text is encoded in some other way. How odd.

The risk: not only that you may reveal information you did not want to reveal, in some cases you may reveal nothing else.

Clive Page, Dept of Physics & Astronomy, University of Leicester

---

## **✶ Check everyone's Vodafone voicemail**

"Andrew Goodman-Jones" <goodie@ozemail.com.au>

*Fri, 11 May 2001 15:29:00 +1000*

With Vodafone Australia if you want to check your voicemail from a public phone (because your battery has gone flat) you just dial your own mobile number and then interrupt the voicemail greeting by pressing \* for the menu. It then asks for your security code.

What is my voicemail security code? I called Vodafone to ask. After they verified it was me (by a phone password) they told me that if I had never set it, the default password is 3333. Another girl in the office next to me just tried hers also and it did the same thing.

The risk? Need to check on your friends', your ex's, your boss', your children's voicemail?

---

## ✶ Car 54, where are you?

David Lesher <wb8foz@nrk.com>

*Fri, 11 May 2001 00:47:14 -0400 (EDT)*

Today's Washpost had a followup to the story of a tourist stricken at the FDR Memorial on the Mall.

<http://www.washingtonpost.com/wp-dyn/articles/A6959-2001May9.html>

It seems DC 911 was unable to process the call because the US Park Police on the scene had no street address for the Memorial. The 911 system didn't know how to find a major feature on the Mall. (They've now added entries to the system for at least some landmarks...)

As a result, the victim waited for 30 minutes (and had to be defibrillated at the scene) before a USPP helicopter finally came & picked him up. (The pilot clearly knew where FDR is sitting..)

The Risk? We have replaced local dispatchers & their knowledge of geography, with a dumb database of finite size, staffed by people many miles away. That database assumes every reported location has a \*known\* address. That's far from true; anyone know a street address for a Metrorail station, or the T in Boston? (Irony: the emergency airshafts on Metro \*do\* have posted addresses!) And Richard Jewell had a similar problem in Atlanta while trying to report that bomb.

Another angle: Can your 911 PSAP accept a lat/long from someone hurt in an accident on a rural road, but with a GPS? I've read accounts of those who gave up trying.

Moral: Your database better be prepared for exceptions...  
like Les Ernest's race declaration.

---

## 🚩 Euro risks, part 1

PvK <paul@sumatra.nl>

Sat, 5 May 2001 14:49:29 +0200

The final step in the introduction of the Euro in most of Europe is imminent. There are just eight months left until, in a major operation surely to involve lots of chaos, national currencies will be exchanged for Euro coins and paper money. The introduction of Euro currency is the last step in a process that was officially started on 1 January 1999 when the exchange rates between the various currencies comprising the Euro were fixed. Banks, stock exchanges and multinationals were quick to convert and have been doing business using Euros for over two years. This gradual introduction, where transactions in both local currency and Euros are intermingled gives rise to interesting errors. This is the account of the first one of many I have run into and of many more that are yet to occur in the year to come.

When I am in France, I regularly dine out in a lovely restaurant called Le Burgonde, in Nolay (Bourgogne). This January I picked up a discarded credit card receipt off the garage floor (I am very sloppy with those little pieces

of paper). The slip contained the payment of our last family visit to the restaurant and was for the grand total of FFr 3500 (about USD 490), which is pretty steep considering the restaurant doesn't even have one Michelin star. I checked my credit card statements at home and it turned out that the restaurant bill was first debited for 560 Euro and later corrected to 560 FFr. Thursday I asked the 'patronne' about this error and the correction. She explained to me that in preparation for the Euro the restaurant was provided with a new card machine that can switch between francs and euros. She showed me how this works. The keypad of the card reader has a number of unlabeled coloured keys. The yellow one, which is the apparently correction key has a convenient second function that switches the machine between francs & euro modes. Of course it's a key that can easily get pressed by accident when you pick up the reader from its cradle. The patronne said that when she complained to the credit card company to have them correct the erroneous transactions, they confirmed that they have thousands of such errors every day.

Paul van Keep

---

## **✶ Euro risks, part 2**

PvK <paul@sumatra.nl>

*Sat, 12 May 2001 11:51:01 +0200*

The reality of the Euro is less than eight months away. So you'd expect companies, who have been allowed to use the Euro since 1999 would be used to it by now. But the opposite is quite true. My company (Sumatra) started pricing it's products in Euro two years ago. Although our accounting was still done in guilders we mailed out invoices using the Euro as the base currency and added prices in dutch guilders as well. The problem is that the Euro amount is only slightly less than half the Euro amount, so a lot of our customers entered the wrong value in their systems and paid less than half or what they owed us. We managed to improve things for a while by adding a big bubble graphic pointing to the Euro total on the invoice containing the text 'Bedrag in Euro' . However since the start of this year things got worse again. We decided to be smart and not wait for the last moment; so we switched our whole accounting over to the Euro on 29 december 2000. We now no longer send invoices in two currencies but in Euro only. Of course the old problem immediately returned. One customer whom we invoiced for EUR 1190 paid only EUR 540. This confusion is currently rampant throughout the E.U. The chances of this happening in Spain or Italy, where there are respectively two and three orders of magnitude between local currency and the Euro, are very slim. But especially in Ireland, Germany and the Netherlands where the difference is small (0.7, 1.9 & 2.2) a lot of incorrect payments are made. A quick guesstimate reveals enormous costs as a result of these errors. About 20% of the companies have switched

to Euro based accounting. Just taking the three countries mentioned above there are close to 300.000 companies invoicing in Euro. Lets assume that 1 in 20 payments are wrong on, say, 500 invoices a year. At a cost of 8 euro per error to correct, the cost over this year alone must be at least EUR 60M.

Paul van Keep

---

## ⚡ Thieves R Us

Mike Godwin <mnemonic@well.com>  
*Fri, 11 May 2001 14:36:51 -0400*

[From David Farber's IP distribution]

Thieves R Us: Computer makers are building equipment on the assumption that we are all copyright outlaws  
Mike Godwin, The American Lawyer, 18 Apr 2001

Every year or two I upgrade to a newer, faster Mac laptop, and this means I go through a now-familiar ritual of hooking up the new machine to the old one through a cable or local area network and copying everything -- software, data (including my MP3 music collection), and settings -- to the new machine. So you can imagine my surprise and horror when I heard reports recently that a new standard for consumer hard drives would make this kind of copying difficult or maybe even impossible.

The reports may have been at least partially wrong, as it turns out. But I

think they raise important issues, and ones we ought to be thinking about now.

The notion that hard drives might be hard-wired to prevent copying first collided with my consciousness in January. That's when I heard about a technology known as CPRM, which stands for Content Protection for Recordable Media. It's being developed by an industry group known as The 4C Entity, with the backing of IBM, Toshiba, and Matsushita.

CPRM, it turns out, was the basis of a flood of criticism against The 4C Entity after a single news story appeared in December in a British online computer journal called The Register. Titled "Stealth Plan Puts Copy Protection Into Every Hard Drive," the article began with an arresting lead: "Hastening a rapid demise for the free copying of digital media, the next generation of hard disks is likely to come with copyright protection countermeasures built in." Okay, that got my attention.

The article went on to say that standard-setting bodies were being asked to adopt CPRM for hard disks. Each disk would have a unique identifier that would help prevent unauthorized copies. The article suggested that this padlock could be built into drives as early as this summer.

The reaction was quick and harsh. By the next day, computer activists, including millionaire software entrepreneur John Gilmore, had circulated the story to mailing lists and other online forums. Gilmore called CPRM "the latest tragedy of copyright mania in the computer industry." He warned that under the standard, users "wouldn't be able to copy

data from  
[their] own hard drive to another drive, or back it up, without  
permission  
from some third party."

Industry spokesmen were quick to respond that the protesters  
misunderstand  
the technology and that their concerns are overblown. The 4C  
Entity said  
that CPRM isn't even designed or licensed for "generic hard  
disks." It is  
instead meant for use with other digital media, such as MP3  
players and  
writeable DVDs. The group also says the technology will be  
optional for  
computer manufacturers. The standard would simply specify a  
common digital  
signal facilitating CPRM technology, but it would not mandate  
that the  
signal be present and turned on in a device.  
These qualifications have not mollified Gilmore and other  
critics, who  
raise the prospect that technologies like CPRM will push the  
digital  
electronics industry into producing only equipment and tools  
with little  
or no capability for unlicensed copying.

Now, at this point you might say, "So what? What's wrong with  
designing  
hardware in a way that prevents you from breaking the law?"

I think the best answer to this is: Nothing, so long as it  
doesn't block  
you from lawful stuff you need to do. Consider: It's certainly  
possible  
today to build a car that will never go over the legal speed  
limit.  
Perhaps speed-related injuries and fatalities are enough of a  
reason for  
the auto industry to produce low-speed cars. But then it would be  
impossible for drivers to do things they legally have a right to  
do, and

often need to do, such as accelerating safely onto a freeway or accelerating to avoid a road hazard. And a car that can do those lawful things can also break the speed limit. Yet we don't assume that the owner of such a car is a likely speeder.

Put more broadly: Technologies that empower people don't discriminate between good uses and bad. So if we build constraints into our computer systems that prevent infringement, we're also making it impossible for users to engage in all sorts of lawful copying. Except for the most ardent IP hard-liners, most people accept that it is a fair use to make private, personal copies of music and movies. But the proposed standard could prevent that sort of activity.

It's worth comparing these digital rights management technologies to the copy protection schemes that were the rage back in the 1970s and early 1980s -- the first decade and a half of the microcomputer revolution. Back then, plenty of commercial software -- not just games, but also productivity software like word processors and spreadsheets -- was coded to prevent copying.

Routine tasks like backing up a hard drive and migrating to upgraded systems were an incredible chore. With backups in particular, the software discouraged activities that normal, prudent computer users ought to be doing. As you may remember (and certainly can imagine), this caused a lot of users to gripe.

Some developers responded by creating programs that circumvented

the copy protection. In the long term, however, most software vendors moved away from copy protection altogether; they began to rely on copyright enforcement and the customers' needs for support and upgrades to protect their interests. You generally need to own licensed copies of software in order to get support when you have problems.

The vendors also began lowering the price of software so that it seemed both reasonable and equitable to pay for it rather than copy it. The primary reason that software vendors moved away from copy protection schemes is that they were confronted with competitors that offered similar products without copy protection and with lower prices. In other words, market forces (Microsoft was not yet considered a monopoly) pushed software companies into more rational setups and better relationships with their customers.

But if copy protection is built into standard computer storage devices, whether hard drives or anything else, what competitors will I be able to turn to? Even my Macintosh PowerBook, which you might think is free from standards imposed in the Wintel world, relies on an IBM standard-issue hard disk.

There's another complication. The Digital Millennium Copyright Act expressly outlaws the dissemination of tools that can be used to circumvent technologies that control access to, or copying of, copyrighted works. I can't even circumvent those technologies myself. Courts have said

that it's illegal even when the underlying purpose of the copying (fair use for a classroom presentation or permitted by license) is lawful. Even if the license of my word processor allows me to make archival copies of the software, it's still illegal for me to use circumvention tools to do so.

This combination of law and hardware means that there's a real possibility that someday soon I won't be able to choose between computer products that employ such schemes and those that don't. If that day comes, I don't know how the market will respond, but I know how I will. To the extent possible, I'll stop buying new computer equipment altogether. I'm guessing at least some other computer buyers will make that decision, too.

This will mean I won't have the fastest and best computer equipment anymore, but I'm betting I can stay afloat by haunting used-computer stores for a long time to come. And I'll have the pleasure of knowing that the computer equipment, MP3 device, or CD burner, etc., that I'm buying doesn't have built into it the assumption that I'm a copyright infringer.

Mike Godwin is chief correspondent of IP Worldwide. His e-mail address is [mnemonic@well.com](mailto:mnemonic@well.com).

[For IP archives see: <http://www.interesting-people.org/> .]

---

**✶ Re: Citibank's meaningless privacy notice (Prevelakis, [RISKS 21.38](#))**

Zygo Blaxell <zblaxell@genki.hungrycats.org>

*Fri, 11 May 2001 15:46:21 -0400*

In other words, what you are saying is "information can be shared with group A when box B is checked and group C when box B is not checked, therefore information can be shared with group A or C regardless of the state of box B." That is true if and only if groups A and C have exactly the same membership.

It is easy to get trapped in logical fallacies if one does not include the legal context of contractual agreements in the analysis.

In reasonable jurisdictions(\*), there are two classes of third parties: those that Citibank can unconditionally share information with (e.g., law enforcement officials), and those with whom Citibank cannot lawfully share information without your permission. Checking boxes on the appropriate form would seem to be a reasonable indication of your desire to grant or deny such permission, which would affect the legal status of certain third parties.

Indeed, quoted sections of the Citibank agreement would seem to acknowledge that this is the case, although other sections of the document would seem to contradict this. The Citibank privacy agreement seems to be written in no language I can understand, whether legal, plain, or otherwise...

(\* ) Of course, I'm not making any assertion about whether Citibank is

actually located in a reasonable jurisdiction...

---

## ✦ **Re: Using calendar reminder service ... ([RISKS-21.37](#))**

Nikita Borisov <nikitab@CS.Berkeley.EDU>

*Fri, 04 May 2001 09:06:46 -0700*

That reminds me of a story a friend of mine told about sixdegrees.com. For those who don't remember the service, it would allow you to enter a list of people you know, as well as how you know them (friend, coworker, brother, etc.), and then let you communicate with people who are two or three levels away from you. A few days after she broke up with her boyfriend, she was looking at her user preferences and decided to update them to reflect this fact. Imagine her surprise when the sixdegrees cheerfully told her that the following message had just been mailed to her ex-boyfriend:

This is a notification that [my friend's name] has cancelled your status as boyfriend.

The RISKS? Lending very personal information to a company and assuming that they will not do anything undesirable with it.

- Nikita

---

## ✦ **RE: MSN "upgrade" creates long distance calling ([RISKS-21.32](#))**

"Bob Frankston" <rmf2gRisks@bobf.Frankston.com>

Sat, 5 May 2001 00:16:04 -0700

The real risk here is a legacy of open loop signaling. In this case, the billing algorithm is implicit -- there is no protocol that allows one to determine and manage the costs of connectivity.

We see the same kind of problem when area codes are split instead of overload -- ones infrastructure changes invisibly and, for the user, perversely.

These were all designed in a more naive era when it was assumed that every action had a human in the loop. What used to seem like clever ideas such as using 1 to mean a toll (charge call) or 900 to charge to a special card "card" (ones phone bill), now seem like kludges.

This is isn't to pick on the phone company. We see the same thing when a part number code has implicit semantics.

And, alas, the DNS is a flashpoint here -- a modern example of old thinking that rolls together disparate mechanisms.

The risk is in carrying old thinking ahead while the world changes. It's the antithesis of many of the "Risks" entries in that it comes from not embracing or, at least, understanding technology. Not so much the artifacts of technology but the concepts underlying it.

There is a technical term for things that go bad because of external changes - bit-rot. (not to be confused with bitrot, the gait of

a semi-horse).

Autocatalysis is a related technical concept.

Bob Frankston <<http://www.frankston.com>>

---

## ⚡ Risks of not monitoring field-deployed systems

John Connor <connjoh@statcan.ca>

*Fri, 04 May 2001 09:32:15 -0400*

Here in Ottawa, we have an extensive bus system with many large bus stations along the routes - kind of like a poor man's above ground subway. In these stations, there are TV monitors with a display showing the number of minutes until the next bus comes, with one line of information for each of the several routes serving that station.

Recently, while passing by one of these monitors, I noticed that it had a Windows-style pop-up box showing. This box was in turn covered by another pop-up with a complaint from Dr. Watson that it couldn't write to some file. The monitor remained in this condition for several days, leading our group here at the office to conclude that there must be a PC in a closet at the station that was in need of some attention, rather than the monitors being driven from some central computer. Probably simply clicking on the OK button on the second pop-up would clear the error boxes.

Two weeks later, nothing has changed, the pop-ups are happily burning

themselves into the monitor. I'm entertaining myself now watching to see when it finally gets fixed. (Is this what they mean by a bus error?)

The risk? Deploying a field system that should work 24/7 with (apparently) no way of remotely monitoring it so that you know if it has failed, and requiring someone to physically go and visit the machine in order to just click a mouse to remedy an all too predictable error condition.

---

## ✶ Re: UPS Shutdown (Borg, [Risks-21.36](#))

Diomidis Spinellis <dds@aueb.gr>

*Fri, 04 May 2001 09:03:13 +0200*

In [RISKS-21.36](#) Kent Borg noted that his UPS failed to power his server when the mains power was restored. The problem can probably be attributed to the way Kent installed and used the UPS rather than the UPS design. To power-down a UPS after its batteries signal that they are close to empty by expecting it to switch-off when the batteries are completely drained is incorrect due to a number of subtle race conditions (another risk).

Consider first of all the scenario expected by Kent:

1. Mains power is interrupted
2. Computer is now powered by the UPS
3. UPS batteries signal a low condition
4. Computer gracefully halts
5. UPS dies as batteries are completely drained
6. Computer switches off as UPS power is interrupted

7. Mains power is restored
8. Computer restarts

Consider now the first race condition: mains power is restored between steps 4 and 5. The UPS will restore power and the computer will wait idly in its halted state. One can counter, that many computers have automatic power management so that (in step 4) they can be shut off instead halted; when power power is restored the computer will correctly restart. Enter now the second race condition: power is restored DURING the shutdown sequence (this sequence can last for several minutes on servers running database applications). The computer will now complete its shutdown sequence and switch itself completely off despite being fed with mains power.

How can one handle these problems? The communication protocol of most UPSs supports a software command to switch-off the UPS. Thus the last action of step 4 is to soft switch-off the UPS (and consequently the computer). When power is restored both will correctly restart.

Note that the implementation of this sequence is not trivial: the UPS software I am familiar with, operates as a user process; when the computer is ready to halt, user processes have died and filesystems are unmounted making it difficult to send that last command to the UPS.

### Conclusions

- 1) UPS software is not optional (if you are searching for an implementation have a look at the open-source Network UPS Tools - NUT <<http://www.exploits.org/nut/>>).
- 2) The correct installation of UPS software is not trivial.

Diomidis Spinellis <<http://www.eltrun.aueb.gr/dds/>>

---

## ⚡ Re: UPS Shutdown (Borg, [Risks-21.36](#))

Chris Smith <[smith@interlog.com](mailto:smith@interlog.com)>

*Sun, 6 May 2001 17:22:37 -0400 (Eastern Daylight Time)*

> the Kent who is now in the market for a UPS with  
> a simple hard power switch that will stay "on".

This feature may be somewhat difficult to find.

Even a simple risk assessment of such a feature makes it look like a really big Risk. If the UPS can't recharge until power returns, but it immediately allows the attached equipment to start up, then there is a high possibility that just a few moments later the main power will drop out again, leaving the UPS unable to provide backup power and allowing the attached equipment to suffer an immediate power loss with no warning.

I can't find a recent reference for this fact, but the idea still seems to make sense - the most likely time for power to cut out is just after it came back on. At one time I ran a PC as a power monitor (yes, letting it fail and restart), and this was a consistent pattern. Major outages were often preceded by several small ones, and also sometimes followed by small ones. Completely standalone outages were rather rare.

Perhaps a Risks reader with more power industry background can supplement my

limited experience.

The bigger lesson seems to be that power security, like data security, is a process. It is a Risk not to treat it as such.

Alternatively, perhaps he can find a UPS which will restart the attached equipment AFTER it recharges.

Chris Smith

<smith@interlog.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 21: Issue 41**

**Wednesday 23 May 2001**

## Contents

- [A Hard Left-Cruise Ship's Autopilot blamed for sharp turns](#)  
[Kelly Bert Manning](#)
- [Another backhoe reminder](#)  
[Bernd Felsche](#)
- [New Bell Canada service: free calls](#)  
[Dave Isaacs](#)
- [The Faith-Based Missile Defense](#)  
[What's New via David Farber](#)
- [Time to bury proposed software law](#)  
[Dan Gillmor via Monty Solomon](#)
- [NZ Electoral Web Site](#)  
[Richard A. O'Keefe](#)
- [Osprey, cont'd](#)  
[Peter B. Ladkin](#)
- [Our software is \\*never\\* wrong](#)  
[Erann Gat](#)
- [Risks in scuba equipment](#)  
[Carl Page](#)
- [More on that college network/spam](#)  
[Danny Burstein](#)

- [Apple Powerbook 'bomb' shuts Burbank airport](#)  
[Monty Solomon](#)
  - [Re: Space Station software problems predicted four years ago](#)  
[Bob Frankston](#)
  - [The new Taiwan \\$1000 bill got the globe backwards](#)  
[Dan Jacobson](#)
  - [Police frequencies and fake calls](#)  
[William Colburn](#)
  - [Power safety](#)  
[Marcus L. Rowland](#)
  - [Ship to Internet](#)  
[Donn Parker](#)
  - [2002 ACM Symposium on Applied Computing: SAC '2002](#)  
[Cliff Jones](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

## ✶ A Hard Left-Cruise Ship's Autopilot blamed for sharp turns

Kelly Bert Manning <bo774@freenet.carleton.ca>

Mon, 21 May 2001 13:06:10 -0400 (EDT)

Over 70 people were injured, 13 requiring treatment, when the ship docked in Victoria, British Columbia. Some refused to get back on board but did so after the US Coast Guard investigated and cleared it to continue without using the autopilot. Two injured passengers remained in Victoria for care.

[http://www2.mybc.com/news/fs.cfm?source\\_id=CP&id=851308](http://www2.mybc.com/news/fs.cfm?source_id=CP&id=851308)

"It was like the Titanic. People were flying around in chairs. The gift shop was destroyed." USA Coast Guard Lt. j.g. Scott Casad is reported to have said that the autopilot malfunction appeared to have been

caused by a  
computer error. The investigation will also look into whether  
the  
autopilot should have been used in the Strait of Juan de Fuca.

It will be interesting to see exactly what sort of "computer  
error" this  
was. A crew member disengaged the autopilot after the second  
turn.

---

## ✂ Another backhoe reminder

Bernd Felsche <bernie@innovative.iinet.net.au>

*Fri, 18 May 2001 10:48:03 +0800 (WST)*

[from <http://www.abc.net.au/news/newslink/nat/newsnat-18may2001-35.htm>]

Telstra [Australia] estimates 50 to 80 per cent of customers  
affected by yesterday's phone outage in New South Wales have  
had  
their phone services restored and says the remainder should be  
fixed  
very soon.

Technicians have worked through the night to fix a cable which  
was  
severed by a backhoe on the central coast yesterday, cutting  
phone  
services from North Sydney to the Queensland border.

Initially,

Telstra hoped to have the cable repaired early yesterday  
afternoon

but the company says the damage was worse than first thought.

Spokesman Paul Levins says the delays are due to the complex  
nature

of the cable repairs. "Inside the encasement are thousands of

tiny

hairlike fibre optics," he said. "It's like knitting each one of

those back together, it is like microsurgery and it is highly technical. But they've got to get the sequencing right so you don't end up attempting to ring your mother down the street and wind

up at the pizza shop."

Bernd Felsche - Innovative Reckoning, Perth, Western Australia

---

## ⚡ New Bell Canada service: free calls

"Dave Isaacs" <davei@ottawa.com>

*Mon, 21 May 2001 13:56:06 -0400*

According to an articles in \*The Toronto Star\* and \*Wired\* (<http://www.wired.com/news/business/0,1367,43967,00.html>), Bell Millennium payphones users were given a rare treat last week: free access to Telehop's Dialaround low-charge long distance service.

A glitch in the access software allowed anyone who entered 10-10-620 into a Bell Millennium pay phone to make unlimited free calls to anywhere in the world. Word spread quickly on Internet newsgroups, until people were literally camping out by the phones to wait their turn.

It is interesting that the hole was known by the public for 6 days before it was fixed. Why the delay? Did it take 6 days to discover the problem?

According to the article, Bell didn't start monitoring the network closely until [a] store containing the pay phones called to complain

that the crowds  
were disrupting their business. I also wonder if Bell and  
Telehop knew  
about the problem for some time, but did not count on the  
exploit being  
described on the Internet.

Dave Isaacs

[Also noted by Aaron Poof Matthews. PGN]

---

## ✈ The Faith-Based Missile Defense (What's New for May 11, 2001)

David Farber <dave@farber.net>

*Sat, 12 May 2001 21:27:17 -0700*

### 1. WEEKLY DISASTER REPORT: THE FAITH-BASED MISSILE DEFENSE

Last week, you will recall, President Bush called for a global  
missile  
shield, including space-based elements, but he was pretty short  
on specifics  
(WN 4 May 01). This week, Defense Secretary Donald Rumsfeld  
called a press  
conference to talk about military uses of space. Many of us  
expected he  
would fill in some of the missing details from the President's  
speech. He  
didn't. Rumsfeld devoutly believes that an effective missile  
defense is out  
there somewhere, but neither he nor the President seems to have  
any idea of  
what the shield would involve or any evidence that such a thing  
is even  
feasible, much less what it would cost, when it might be  
deployed or whether  
it even has to work. Rumsfeld wanted to talk about the  
management and  
organization of a new national-security space initiative; it

would be given  
the task of filling in the missing details. Not a bad strategy  
-- opponents  
of a missile shield are left with nothing specific to attack.

[For IP archives see: <http://www.interesting-people.org/> ]

---

## ⚡ Time to bury proposed software law (Dan Gillmor)

Monty Solomon <monty@roscom.com>

*Sun, 13 May 2001 18:14:02 -0400*

UCITA, the ``Uniform Computer Information Transactions Act,' ' is  
the  
technology industry's version of Dracula. It's designed to suck  
money from  
overmatched consumers, and it keeps emerging from the coffin.  
Just about  
every serious pro-consumer official and organization has  
denounced UCITA, a  
proposed uniform state law that would tilt the balance in  
software  
transactions strongly toward the seller. But UCITA's backers,  
mostly in the  
computer industry, are not giving up -- and they may be on the  
verge of  
getting help from key public officials who, acting in good  
faith, would harm  
the people they're sworn to protect. [Dan Gillmor, Time to bury  
proposed

software law, \*San Jose Mercury\*, 13 May 2001

[http://www.siliconvalley.com/docs/opinion/dgillmor/dg051301.  
htm](http://www.siliconvalley.com/docs/opinion/dgillmor/dg051301.htm)]

---

## ⚡ NZ Electoral Web Site

"Dr Richard A. O'Keefe" <ok@atlas.otago.ac.nz>

Wed, 23 May 2001 14:25:42 +1200

There's a saying in Australia and New Zealand: "when the Americans have a 'cute' idea, we wait a couple of years until they've proven that it's really really dumb, and THEN we copy it."

\*Otago Daily Times\*, 22 May 2001, front page.

Voters will be able to enrol on the electoral roll and update their

details online using services on an elections web site.  
Associate Justice

Minister Margaret Wilson said the service would be particularly useful for

people living in remote areas or overseas, as well as the disabled. She

also hoped it would encourage young people to enrol to vote.  
The site is

[www.elections.org.nz](http://www.elections.org.nz).

I just hope the "disabled" people she has in mind are not the ones with poor visual acuity, because in Netscape 4.7x or Amaya on a SPARCstation, the page is unreadable; in Netscape on a Mac it is unreadable, and while it is marginally readable in iCab, it somehow managed to kill iCab.

The site is slow and confusing. I have made repeated attempts today to view my own record, and always arrived at a page saying who was eligible to enrol.

What would anyone reading comp.risks confidently predict would be used to identity a potential voter, so that no-one else can scribble on your record?

SSN (which we call Tax File Number, TFN, and do NOT use except for tax purposes). Nope. It's better than that.

Full name and date of birth.

Maybe the fact that I can't get to my record even with that information is the security feature I was hoping for....

---

## **Osprey, cont'd [Ladkin, [Risks 21.33](#), [21.38](#)]**

"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>  
*Thu, 17 May 2001 07:36:52 +0200*

I advised RISKS readers in [Risks 21.33](#) and [21.38](#) of three documents concerning the troubled V-22 Osprey tilt-rotor development and deployment program - the briefing material from the US GAO review of the program, the briefing transcript concerning the results of the investigation into the December 2000 crash, and the report of the Blue Ribbon Panel appointed by then-Secretary of Defence Cohen to evaluate the program.

The briefers on the accident investigation (the JAG report) into the December crash pointed unambiguously to a software problem, what they called a "software anomaly". They said that the Primary Flight Control System (PFCS) did not behave as it should have (namely, that in a particular situation, it commanded significant control system changes when it should have done "nothing") and that this was due to the software.  
[Ladkin,

[RISKS-21.33](#)]

The Blue Ribbon Panel report devoted less than a page to software reliability. Their recommendations focused on methods effective for determining the characteristics of complex control systems in their operational environment, and did not include certain standard methods for assessing and repairing safety-critical software known to contain errors. [Ladkin, [RISKS-21.38](#)]

Define a software error to be a failure of the software implementation to meet the design specification, or a failure of the software design to meet PFCS requirements. The JAG briefing indicated that a software error had been discovered; the Blue Ribbon Panel report led me to suspect whether this had indeed been the case.

I spoke with Professor Eugene Covert, one of the four members of the Blue Ribbon Panel, on Tuesday, 15 May 2001, and I put to him the argument of my [RISKS-21.38](#) note. Although a significant amount of his information is privileged, he was able to confirm that no software error as above had been implicated in the December accident and that the range of scenarios I suggested in [RISKS-21.38](#) broadly represented likely scenarios for the genesis of the control behavior exhibited.

Peter Ladkin, University of Bielefeld. <http://www.rvs.uni-bielefeld.de>

---

## **✶ Our software is \*never\* wrong**

Erann Gat <gat@flownet.com>

*17 May 2001 09:52:48 -0700*

The other day I got an e-mail from my on-line credit-card company telling me that my e-mail preferences had been updated. Trouble is, I hadn't logged in to my account for weeks, and I could not remember ever setting any e-mail preferences. So my risk radar said, "Hack!" and I called the company.

The rep assured me that my account had not been broken into. How did they know, I asked. "I've got your account right here and I can tell that no one has tried to break in." Yes, but *\*how\** can you tell that? Well, because if someone had tried to break in it would have said so, and it didn't, so no one has.

I explained to the rep about the e-mail that I got which could only be explained by either someone breaking in or a bug in their software. And if there was a bug in their e-mail software there might also be a bug in their hack-detection software. It should come as no surprise that this made little impression on the rep.

---

## **✶ Risks in scuba equipment**

"Carl Page" <carlp@findpage.com>

*Fri, 11 May 2001 20:34:00 -0700*

Scuba divers make a fetish out of safety, for good reason. I found the list of problems identified by testing by this outfit to be instructive, and perhaps generalizable. Thought you might enjoy it for RISKS digest.

<http://www.scubadiving.com/gear/scubalab.shtml>

Revelations: ScubaLab tests have led to many important revelations, including:

- a. A regulator that actually shut off the air supply (a voluntary recall by the manufacturer was initiated).
- b. Regulators that were advertised as upgraded and yet actually had increased work of breathing.
- c. Regulators that could not deliver adequate air flow below 100 feet.
- d. Regulators that were not adequately prepared for use as delivered.
- e. Add-on fittings for regulators, such as swivels, that changed a regulator's performance from acceptable to unacceptable.
- f. BCs that were supposedly improved with new airways or weight systems, but that actually performed worse on tests.
- g. BCs with advertised buoyant lift capacities that were significantly different from the actual values.
- h. BCs with mismatched inflator and ambient hose lengths, disabling the remote exhaust function.
- i. BCs with excessive inherent buoyancy.

- j. BCs with excessive body squeeze.
- k. A dive computer that "lost" four minutes during decompression.
- l. Dive computers that allowed continuous deep bounce diving.
- m. Dive computers that caused compasses to read incorrectly.
- n. Hoseless dive computers that lost their signal when other electronics were used.
- o. Dive computer PC interfaces that did not work.
- p. Dive computer instructions that were not correct.

Setting the Record Straight

---

## 🔥 More on that college network/spam (tls, [RISKS-21.39](#))

danny burstein <dannyb@panix.com>  
*Fri, 11 May 2001 22:16:48 -0400 (EDT)*

In [RISKS-21.39](#), of 11-May-2001, your correspondent, tls@panix.com, discussed the problems with the way a local university had recently set up an open 802.11 (wireless) network.

He commented that while this was an arguably defensible decision for a university, he was quite concerned about its potential use by spammers. To quote him:

> The RISK? Their campus mail-handling machines will relay mail to

> any inside or outside destination if it's received from an  
address  
> "inside" their campus network. The network architecture  
they've  
> chosen for their wireless deployment dictates that anyone can  
walk  
> onto their (large, urban) campus, or even just park his car  
outside,  
> and spam away freely with hundreds of megabits per second of  
> bandwidth to most points on the Internet.

Having tried exactly what [tls@panix.com](mailto:tls@panix.com) describes (except that I  
sat in an  
air-conditioned van and only sent some test messages...). I can  
confirm  
that this university's mail servers work as he fears.

Furthermore, any mail coming through them will have an envelope  
indicating  
it came from a well known and trusted source. Meaning not only  
would people  
be more likely to let it through their filters (whether  
computerized or the  
Mark One Eyeball method of glancing at the "from" and "subject"  
line), but  
they're also far more likely to open it.

Meaning this type of service can easily be used to spread all  
sorts of  
nastiness. And not just limited to e-mail viruses and trojans.

Getting back to spamming: this system doesn't block outgoing  
"port 25"  
access, meaning a spammer could set up their own mail server and  
pseudo-anonymously engage in all sorts of socially deviant  
activities.

The RISK? If you leave your front door open on the Internet,  
you're  
leaving everyone else's front door ajar.

## **Apple Powerbook 'bomb' shuts Burbank airport**

Monty Solomon <monty@roscom.com>

Sun, 13 May 2001 18:11:09 -0400

<http://www.theregister.co.uk/content/2/18438.html>

Apple Powerbook 'bomb' shuts airport, article by Drew Cullen, 23 Apr 2001

A California airport was closed for six hours [20 Apr 2001], following a bomb scare. And the 'culprit'? Step forward the Titanium Powerbook G4. Operators of an x-ray machine installed at Burbank airport were unable to get a high-enough res look at a machine trundling through security. They called in back up for some chemical analysis. Swabs revealed "residues" which caused some concern The police and the FBI were called in, flights were cancelled, and hundreds of customers were left milling the booking hall.

After six hours, the police determined that the Powerbook was indeed a Powerbook and not a bomb - its hapless owner was released from questioning, and the airport was free to return to its business.

The scare was blamed on the titanium used in the laptop casing - officials said this could have given a false reading

Let's hope this mix-up had something to do with the x-ray machine, rather than some magical shielding properties possessed by the Titanium PowerMac G4. If somehow it's the latter, Apple could have an awful lot of product liability suits on its hands.

## ✈ Re: Space Station software problems predicted four years ago

"Bob Frankston" <rmf2gRisks@bobf.Frankston.com>

Sat, 5 May 2001 00:16:09 -0700

(Gross, [RISKS-21.39](#))

Given that I'm in a plane and have time to catch up on old reading (but not follow URLs -- at least until Boeing deploys their IP-to-the-Seats infrastructure!), I might as well continue to take the contrarian role and defend the value of risk. There is no way to escape risk so might as well revel in it.

In this case, I can't resist wondering how one can debug complex software before deploying it. The danger is more in assuming one can and not preparing for failure than in not doing complete debugging. This doesn't mean one should not do any testing, just that the limits must be recognized.

I'm a great admirer of MIR -- the ability to keep it going with just the "chewing gum and bailing wire" (to use an old metaphor) impresses me more than a design which is "perfect".

In general those who can experiment and survive have a major advantage over those who must put their energy into trying to avoid risk. If one never fails, one never succeeds.

In the case of the Space Station, the real question is how the overall

system is architected. Do point failures propagate or are the quenched? What are the fallback procedures? Is there an attempt at efficiency that tends towards depending on each module doing what it is supposed to do or is there the necessary mutual distrust.

I fear that a procurement process that is overly specific actually increases the risk by making it more difficult to learn by doing.

Bob Frankston Curmudgeon@Bobf.Frankston.com <http://www.Frankston.Com>

---

## ✶ The new Taiwan \$1000 bill got the globe backwards

Dan Jacobson <jidanni@kimo.FiXcomTHiS.tw>  
*19 May 2001 08:41:52 +0800*

The day I discovered this error, the chief had to call two press conferences the same day to deny it. If he admitted it, then he would have had to recall all the bad bills and print new ones (I suppose not to confuse counterfeit detection systems). It would not be possible to admit errors without revising the note.

<http://www.geocities.com/jidanni/1000xinxintaibi.htm>

<http://www.geocities.com/jidanni> Tel886-4-25854780

---

## ✶ Police frequencies and fake calls (Re: Hutto, [RISKS-21.39](#))

Schlake (William Colburn) <schlake@nmt.edu>

Sat, 12 May 2001 15:32:55 -0600

I am a volunteer Field Coordinator for the New Mexico State Police (District 11). The Albuquerque Metropolitan area (District 5 SP) has been plagued by problems like this, but from cell phones and FRS (Family Radio Service) radios, not on police frequencies. Even so, police frequencies are nothing special.

The quote "The police department's emergency radio system uses two sets of security identification codes and a computer to prevent unauthorized access." sounds like media hype to make it sound like something special was done. All police frequencies are well known, they are available from the FCC web page. The "identification codes" are most likely the sub-audible tones which tell the repeater how to process the signal. These are also well known. If I were to take my radio to Denver, I could probably be operating on their frequencies within a matter of minutes.

The "modification" of the radio is also media hype. Almost any radio, except those purchased from Tandy, can be modified without any effort. You open the back of the radio, and (in most major brands) you will see a single copper wire amongst preprinted circuit boards. Anyone want to guess what happens if you cut the wire? The FCC laws require commercial radios to be fixed frequency. These laws were made for crystal radios, and shouldn't be on the books anymore. Most manufacturers make one radio, and

just pack and  
wire it differently in different cases for different  
applications.

The computer is most likely just the data link between the cars  
and the  
dispatcher that uploads and downloads information to the in car  
computers.

As for bogus radio calls, we have had a veritable plague of fake  
distress  
calls from FRS radios and cell phones. Most cell phones will  
call 911  
without a service provider or SIM card, which allows anonymous  
untraceable  
crank calls. SAR teams and emergency personnel have responded  
to crashed  
airplanes, automobile accidents, lost hikers, and lots more.  
They solved  
this problem by asking for a phone number that they can call to  
verify the  
callers identity. One real hiker was saved because he referred  
us to the car  
company that he rented his car from. A woman "lost in the  
mountains" was  
ignored because she wouldn't give her name, a name of a friend  
or relative,  
or a phone number where anyone who knew her could be contacted.

---

## **⚡ Power safety ([RISKS-21.36](#))**

"Marcus L. Rowland" <mrowland@ffutures.demon.co.uk>  
*Sat, 12 May 2001 23:28:24 +0100*

I said

>A couple of years ago we rebuilt two labs and were able to  
replace two

>of these units with normal earth leakage and circuit breakers;  
there  
>has since been no trouble, nobody has been electrocuted, and we  
have  
>never had any loss of power in those labs. I'm now trying to  
get the  
>rest replaced.

And as if by magic I've just heard that they're going to be  
fixed in the  
next holiday, apparently because my complaints finally convinced  
the  
school management that the cure is worse than the disease. Many  
thanks  
to everyone who made suggestions on this in e-mail.

One point did arise in several messages, a suggestion that we  
have  
separate ring mains put in for the computers. Apart from  
expense, there  
was a serious safety issue with this; as mentioned in the  
original post,  
the room is running with the electrical supplies at about -110v  
negative, +110v positive, rather than the 0 negative, 220-230v  
positive  
of normal UK ring mains. If a separate supply was put in it  
would run at  
the normal voltage, and possibly a different phase, which could  
lead to  
much more serious problems if the two systems were ever linked.

Marcus L. Rowland

---

## Ship to Internet

Donn Parker <Donnlorna@aol.com>  
*Sat, 12 May 2001 09:27:36 EDT*

Some cruise ships (Renaissance R Two) now have Internet cafes

using  
satellite services. I was able to do all of my e-mail work 24/7  
for two  
weeks (\$100 fee) in the Mediterranean from Venice to Barcelona  
-- except for  
one day in Naples Harbor. On that day, the ship was in a  
position that  
precluded the dish line-of-sight to the satellite. The funnel  
was in the  
way. I received no refund. Donn Parker (retired in the nick of  
time and  
glad of it).

[That would be known as A Napoli Day. Clearly, A Napoli Day  
Keeps the  
Internet Away. But there should also be a Napoli Woods in  
honor of the  
late movie actress. PGN]

---

## **2002 ACM Symposium on Applied Computing: SAC '2002**

Cliff Jones <cliff.jones@ncl.ac.uk>  
*Mon, 21 May 2001 10:24:49 +0100*

2002 ACM Symposium on Applied Computing (SAC '2002), CALL FOR  
PAPERS

Madrid, Spain, 10-13 March 2002

Special Track on Inter-disciplinary Approaches to the  
Design

of Dependable Computer-Based Systems

<http://www.dai.ed.ac.uk/homes/rnp/sac2002/cfp.html>

All submissions must be received by September 1, 2001.

A special track on inter-disciplinary Approaches to the Design  
of Dependable  
Computer Systems will be held at SAC'2002. Society's dependence  
on  
computer-based systems continues to increase. The systems

themselves --  
embracing humans, computers and engineered systems - become ever more  
complex as they feed an insatiable appetite for new and extended  
functionality. Furthermore, these trends coincide with pressure  
for systems  
to be brought to market faster and at lower (and more  
predictable)  
cost. Achieving sufficient dependability in these systems, and  
demonstrating  
this achievement in a rigorous and convincing manner, is of  
crucial  
importance to the whole fabric of the modern Information Society.

Although progress has been made in achieving high dependability  
in computer  
hardware and software, wider systems involving computers, people  
and business  
or social organisations are often disastrously unsuccessful and  
the cause of  
huge financial losses or worse. It has become clear in recent  
years that  
satisfactory resolution of this situation demands an inter-  
disciplinary  
approach targeted at understanding the fundamental problems that  
arise in  
attempts to build systems involving complex interactions amongst  
numbers of  
computers and human beings. Inadequate understanding of the  
complete  
organisational and cultural context of use is often a  
significant cause of  
lack of dependability of major new computer-based systems, and  
will be a  
major focus of this track.

By bringing together computer scientists, psychologists and  
sociologists who  
share an interest in the problems of dependability, the proposed  
track will  
make an important contribution to fostering this inter-  
disciplinary approach.  
Submissions will be invited on (but not limited to) the

following themes:

- \* Architecture and organisation of systems, processes and their environment, e.g., use of diversity in systems and processes
- \* Work and its relationships with technological systems and artifacts, e.g., collaboration and interaction, organizational culture and trust
- \* Reasoning about dependability attributes, e.g., temporal predictability and responsiveness of systems and processes, security and confidentiality, formal methods
- \* Socio-technical approaches to systems design and development, e.g., knowledge management and process change, co-evolving work and technologies
- \* Assessment and management of risks involved in system development and deployment

Original papers from the above-mentioned or other related areas will be considered. Each submitted paper will be fully refereed and undergo a blind review process by at least three referees. The accepted papers in all categories will be published in the ACM SAC'2002 proceedings.



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 21: Issue 42

Friday 25 May 2001

## Contents

- [Thought-provoking book on software: David Parnas](#)  
[Jim Horning](#)
- [Software Engineering, Dijkstra, and Hippocrates](#)  
[Michael L. Cook](#)
- [Lost train](#)  
[Debora Weber-Wulff](#)
- [Aimster vs. the recording industry](#)  
[NewsScan](#)
- [Converting Pi to binary: DON'T DO IT!](#)  
[Keith F. Lynch via Russ Perry Jr.](#)
- [``The Wind Done Gone" ban done gone -- with abandon, gone](#)  
[PGN](#)
- [FBI arrests dozens for Internet fraud](#)  
[NewsScan](#)
- [What they know or don't know about you!](#)  
[Monty Solomon](#)
- [EU considers retaining \\*all\\* telecom traffic](#)  
[Dave Weingart](#)
- [CERT subjected to "just another attack"](#)  
[NewsScan](#)

- [Great DoS attack for cell phones](#)  
[Robert Moskowitz](#)
  - [Office XP modifies what you type: Peter Deegan in Woodyswatch](#)  
[via Jonathan Arnold](#)
  - [Weatherbug](#)  
[James Garrison](#)
  - [37% of programs used in business are pirated](#)  
[NewsScan](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

## ⚡ Thought-provoking book on software: David Parnas

Jim Horning <horning@intertrust.com>

*Fri, 25 May 2001 15:20:48 -0700*

Despite a half-century of practice, a distressingly large portion of today's software is over budget, behind schedule, bloated, and buggy.

To those who wonder why, and whether anything can be done about it, I have long recommended the book *The Mythical Man-Month*, by Frederick P. Brooks, Jr.

<http://www.amazon.com/exec/obidos/ASIN/0201835959/>

This book has stayed continuously in print since 1975, and remained remarkably relevant.

Now there is another book I would put beside it. A little more technical and less management-oriented, but equally thought-provoking. It is *Software Fundamentals: Collected Papers* by David L Parnas, Daniel M. Hoffman and David M. Weiss (eds.), Foreword by Jon Bentley:

<http://www.amazon.com/exec/obidos/ASIN/0201703696/>

Parnas has been writing seminal and provocative papers about

software and software development for more than 30 years, and this book collects more than 30 of them. It includes well-known classics such as "On the Criteria to Be Used in Decomposing Systems into Modules," "On a 'Buzzword': Hierarchical Structure," "On the Design and Development of Program Families," "Designing Software for Ease of Extension and Contraction," "A Rational Design Process: How and Why to Fake It," and "Software Engineering: An Unconsummated Marriage." It also has some lesser-known gems, such as "Who Taught Me About Software Engineering Research?", "Active Design Reviews: Principles and Practices," and "Software Aging."

Browsing or reading this book, I think you'll be struck with how much of today's "conventional wisdom" about software was introduced (or championed very early) by Dave, and by how many of his good ideas have still not made their way into current practice. (Why?)

Parnas isn't always right, but he's never dull. One of the most valuable things to do with this book is to pick something he says that you disagree with, and try to construct a convincing argument that he's wrong -- you'll probably find it harder than you expect, and you'll almost surely learn something valuable.

Jim H.

PS. Truth in advertising: I wrote introductions for two of the papers, but I don't get royalties.

## ✶ Software Engineering, Dijkstra, and Hippocrates

"Michael L. Cook" <MLCook@collins.rockwell.com>

*Mon, 14 May 2001 17:58:35 -0500*

The March 2001 issue of the \*Communications of the ACM\* contains an article by Edsger Dijkstra called "The End of Computing Science?"

In it, he states "I would therefore like to posit that computing's central challenge 'How not to make a mess of it,' has \*not\* been met."

As many of the RISKS entries have shown, application and other developers have certainly made a mess of things at times, often of Laurel and Hardy proportions ("That's another fine mess you've got us into."), and worse.

If/when Software Engineering becomes a fully licensed profession, perhaps part of the code of ethics should be similar to the intent of part of the Hippocratic Oath, "First, do no harm". This is a paraphrase of the statement "The health and life of my patient will be my first consideration" which is from the World Medical Association's "Declaration of Geneva" of 1948.

Or, as colleague Glen McCort once said in a meeting, "Don't do anything really stupid."

Michael Cook

[There is a big difference between Hippocrates and Hypocrites. In particular, there are quite a few Hypocrites who claim

they are

"Software Engineers" but nonetheless write extremely riskful software. PGN]

---

## ⚡ Lost train

Debora Weber-Wulff <weberwu@fhtw-berlin.de>

*Wed, 16 May 2001 22:38:54 +0200*

I was in Chur in Switzerland last week and read the sad story of the lost train in the local newspaper. They were having trouble with a train that had to be diverted because of technical troubles along the line. Someone made a mistake while entering in the departure times in their tracking system. The system complained, something along the lines of: "You can't enter a departure time that has already passed", but someone pushed "do it anyway", and somehow managed to get the train sent off. They called, manually, each station along the (beautiful and scenic) route to Chur to let them know that the train was coming. No problem, except that someone forgot to tell the penultimate stationmaster. Since he did not know the train was coming, he dispatched the last little train of the evening off to the skiing resort Davos, and was packing up his things to go home when the train came into his station. Imagine his shock! There were still 5 passengers on the train that wanted to get home. Apparently it took quite a lot of discussion before everyone managed to get a taxi home, courtesy of the Swiss National Train

Company. [Rhaetian Railway? See [RISKS-21.44](#). PGN added in archive copy.]

Just goes to show you: If people think they have entered in something correctly, no amount of error messages will convince them otherwise.

Prof. Dr. Debora Weber-Wulff, FHTW Berlin, FB 4, Treskowallee 8, 10313 Berlin  
GERMANY +49-30-5019-2320 <http://www.f4.fhtw-berlin.de/people/weberwu/>

[Not quite Chur-noble, but perhaps Chur-lish. PGN)

---

## **Aimster vs. the recording industry**

"NewsScan" <newsscan@newsscan.com>  
*Mon, 21 May 2001 08:33:35 -0700*

The recording industry may be hoisted on its own petard if the Napster-like music swapping service called Aimster is successful in its legal strategy against the Recording Industry Association of America (RIAA). Unlike Napster, Aimster (which has no central servers to maintain and leaves users individually responsible for their actions) encrypts transmissions, and so there is no way for the RIAA or any other outside party to distinguish between files which are in compliance with copyright law and those that infringe on it. Of course, RIAA could simply decrypt the files -- but then it would be in violation of the Digital Millennium Copyright Act (DMCA), a

law that it strongly supports, and that makes it a criminal offense to circumvent encryption protection of copyrighted material. (\*The New Republic\*, 21 May 2001; NewsScan Daily, 21 May 2001; <http://www.tnr.com/cyberlaw/babbitt051101.html>)

[NB: Correct English usage is: "hoist with one's own petard" (victimized or hurt by one's own scheme) (Webster via PGN)]

---

## **⚡ Converting Pi to binary: DON'T DO IT! (via Russ Perry Jr.)**

"Keith F. Lynch" <kfl@KeithLynch.net>  
{[not] included}

Newsgroup: alt.math.recreational

WARNING: Do NOT calculate Pi in binary. It is conjectured that this number is normal, meaning that it contains ALL finite bit strings.

If you compute it, you will be guilty of:

- \* Copyright infringement (of all books, all short stories, all newspapers, all magazines, all web sites, all music, all movies, and all software, including the complete Windows source code)
- \* Trademark infringement
- \* Possession of child pornography
- \* Espionage (unauthorized possession of top secret information)
- \* Possession of DVD-cracking software
- \* Possession of threats to the President
- \* Possession of everyone's SSN, everyone's credit card numbers, everyone's PIN numbers, everyone's unlisted phone numbers, and everyone's passwords
- \* Defaming Islam. Not technically illegal, but you'll have to go

into hiding along with Salman Rushdie.

\* Defaming Scientology. Which IS illegal -- just ask Keith Henson.

Also, your computer will contain all of the nastiest known computer viruses. In fact, all of the nastiest POSSIBLE computer viruses.

Some of the files on my PC are intensely personal, and I for one don't want you snooping through a copy of them.

You might get away with computing just a few digits, but why risk it?

There's no telling how far into Pi you can go without finding the secret

documents about the JFK assassination, a photograph of your neighbor's six

year old daughter doing the nasty with the family dog, or a complete copy of

the not-yet-released Pearl Harbor movie. So just don't do it.

The same warning applies to  $e$ , the square root of 2, Euler's constant, Phi,

the cosine of any non-zero algebraic number, and the vast majority of all

other real numbers.

There's a reason why these numbers are always computed and shown in decimal, after all.

---

## **⚡ "The Wind Done Gone" ban done gone -- with abandon, gone**

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

*Fri, 25 May 2001 15:03:17 -0700 (PDT)*

Although it is not directly computer relevant, this case is nonetheless

noteworthy in RISKS, where April-Fools' spoofs and parodies are

an old tradition. A U.S. appeals court in Atlanta today overturned a lower-court ruling that Margaret Mitchell's estate could block the publication of ``The Wind Done Gone'', an apparent parody of ``Gone With the Wind'' that is written from the point of view of black slaves. [Source: Karen Jacobs, Reuters, 25 May 2001, PGN-ed]

---

## **⚡ FBI arrests dozens for Internet fraud**

"NewsScan" <newsscan@newsscan.com>  
*Thu, 24 May 2001 09:32:40 -0700*

The Federal Bureau of Investigation has in the past ten days charged 88 individuals with Internet crimes, including wire and mail fraud and money laundering. A government prosecutor said: "Internet fraud -- whether it's in the form of securities and other investment schemes, online auction and merchandising schemes, credit card fraud and identity theft -- has become one of the fastest-growing and most pervasive forms of white-collar crime."  
(Bloomberg News/\*The Washington Post\*, 24 May 2001; NewsScan Daily, 24 May 2001; <http://washingtonpost.com/wp-dyn/articles/A67744-2001May23.html>)

---

## **⚡ What they know or don't know about you!**

Monty Solomon <monty@roscom.com>

*Fri, 11 May 2001 23:39:05 -0400*

When Richard Smith (Privacy Foundation's CTO) obtained his FBI file from Choicepoint in Georgia, he discovered that he had died in 1976, and had had aliases with Texas convicts known as Ricky or Rickie. This is apparently the kind of info that the FBI now depends on. In 1998, a Chicago woman with no criminal record was fired after Choicepoint info mistakenly indicated she was a shoplifter and convicted drug dealer. Choicepoint info was also involved in thousands of Floridians being mistakenly identified as felons and disenfranchised in the November 2000 election. Choicepoint blames that on a data aggregator, DBT.

[Source: Julia Scheeres, What They (Don't) Know About You, 11 May 2001

<http://www.wired.com/news/privacy/0,1848,43743,00.html>; PGN-ed]

[With regard to flagrant data mining of incorrect information,

What's yours is mined. PGN]

---

## **✶ EU considers retaining \*all\* telecom traffic**

Dave Weingart <dave.weingart@us.randstad.com>

*Thu, 17 May 2001 13:14:01 -0400*

According to an article in The Register, the Council of the European Union is considering implementing rules that call for storing all

telecom traffic  
(all phone calls, all Net usage, every e-mail) and making this data  
accessible for at least seven years. This will be done in the name of  
"public safety and law enforcement," no doubt.

<http://www.theregister.co.uk/content/5/19003.html>

Technical considerations aside (the concept of server farms the size of  
France comes to mind), the whole thing is just a dreadful idea.

Dave Weingart, Randstad North America dave.weingart@us.randstad.com  
1-516-682-1470

---

## **🔥 CERT subjected to "just another attack"**

"NewsScan" <newsscan@newsscan.com>  
*Thu, 24 May 2001 09:32:40 -0700*

The Web site of the federally funded Computer Emergency Response Team (CERT) was clogged by a "denial of service" attack that lasted 30 hours this week. CERT, which is located at Carnegie Mellon University in Pittsburgh, has a mission of providing warnings about computer attacks and viruses. An official of the organization said: "We get attacked every day. This is just another attack. The lesson to be learned here is that no one is immune to these kinds of attacks. They cause operational problems, and it takes time to deal with them." [AP/\*USA Today\*, 24 May 2001; NewsScan Daily, 24 May 2001]

<http://www.usatoday.com/life/cyber/tech/2001-05-24-cert-hacked.htm>]

---

## **Great DoS attack for cell phones**

Robert Moskowitz <rgm@icsalabs.com>

*Tue, 15 May 2001 12:35:09 -0400*

(by way of David Kennedy)

Courtesy of the FAA:

The FAA has this neat airport traffic website:

<http://www.fly.faa.gov/flyFAA/index.html>

where you can check out conditions at any airport. Well, recently they added the option to get e-mail on airport conditions:

[http://www.fly.faa.gov/Notify\\_Signup/notify\\_signup.html](http://www.fly.faa.gov/Notify_Signup/notify_signup.html)

with a warning to be careful not to select all airports as that would be a lot of mail.

Now the way this works is you put in an e-mail address and a password. this is the password to make changes on the FAA's site. Then they ask you what airports and how many characters your e-mailer can handle.

I have selected DTW and for days I will get no mail. This morning I have already gotten 3 messages about various delays due to different thunderstorms.

SO if someone does not like someone else, they just set this

system to mail  
bomb the other person's cell phone. Imagine how annoying it  
will be with a  
phone constantly going off and not knowing how to stop the  
mail. would  
most people figure out how to get this stopped? **\*\*I\*\*** have not  
contacted  
my cellular provider on how to stop SMS spam, so I doubt if  
there is much  
experience here. there will be before this year is done.

Robert Moskowitz, Senior Technical Director [rgm@icsa.net](mailto:rgm@icsa.net)  
ICSA Labs, a division of the TruSecure Corporation (248) 968-  
9809

---

## **Office XP modifies what you type: Peter Deegan in Woodyswatch**

Jonathan Arnold <[jdarnold@buddydog.org](mailto:jdarnold@buddydog.org)>  
*Wed, 23 May 2001 15:10:44 -0400*

[From Woody's Office Watch (<http://www.woodyswatch.com>)]

4. IN OFFICE XP, THE LINK YOU TYPE AIN'T WHAT YOU GET  
Remember when I asked you to send me your rants about Office  
XP?

Editor-in-Chief Peter Deegan has a great one:

I didn't believe it when it first happened to me, but now  
Microsoft

arrogantly and shamelessly confirms the bug. When you type a  
hyperlink in

FrontPage 2002, Word 2002, Excel 2002, PowerPoint 2002, or  
Outlook 2002

(using Word as your email editor), the Office application will  
alter what

you've typed, without notifying you or giving you an  
opportunity to undo

the "correction." In fact, in most cases, you can't override the

"correction" at all: you're stuck with FP, Word or Excel's version of what you typed. Tough luck Charlie.

Try it yourself. In Office XP, choose Insert | Hyperlink then type in this

fake hyperlink

<http://www.fred.com/trial//2345/>

Hit enter, and the double slash is unceremoniously converted to a single

slash. You aren't notified. You aren't given a chance to change it. In

fact, with one exception, you can't even \*override\* Office's ham-handed

mangling of your carefully constructed hyperlink.

The exception: in FrontPage 2002 you can fix the link by going into HTML

mode and overtyping - but there's no such option in Word, Excel PowerPoint, or Outlook. Even Microsoft can't suggest a workaround.

It's even worse than you might imagine. The text appears in the document

the way you typed it - that is, you'll see

<http://www.fred.com/trial//2345/>

in your document. But the link itself - the part behind the scenes that

controls where you go when you click on the text - is altered to

<http://www.fred.com/trial/2345/>

without any notice. Don't believe me? Follow these instructions, then

right-click on the hot text and pick Edit Hyperlink. Look in the Address

box. See that?

While a double slash is unusual, it is a valid hyperlink used in the real

world, most commonly as a delimiter between parameters. Microsoft has no

right to arbitrarily change a link I've typed, especially if there's no way to override the change.

We put this problem to Microsoft's PR folks with a series of questions to help clarify the situation. Their response was among the most arrogant and obfuscatory we've seen in many years of dealing with the company - a dismissive response not designed to help or reassure prospective Office XP purchasers. In fact, it has only made a bad situation worse.

Microsoft says it's not an issue at all! The change is done intentionally for (you gotta love this) "cleanliness and consistency." Oy. Apparently the accuracy of a hyperlink is secondary to it looking nice.

Microsoft dismisses the double-slash change problem saying they "don't know of any servers which deal with a double slash in the path component any way other than to treat it as a single-slash". C'mon. Call 1-800-GET-A-CLUE guys. Double slashes are used all the time. More than that, it isn't Microsoft's job to decide whether the URLs I type are politically correct.

Microsoft goes on to say "some older servers did not like to have the double-slashes in the path and had difficulties with double slashes."

Well, OK, that may be true but there are plenty of other typing errors that can make a link break. Double-slashes may be a problem in some cases, but in others they are necessary.

I really wanted to hURL when the 'Softies said, "we don't change the

parameter data, only the path part of the URL." Good grief. This comes from a company that assumes everyone uses the Microsoft method of passing information through links. In the Microsoft world you pass data to a web page by adding a question mark to the end of the link then adding the variables. Incredibly, not everyone uses Microsoft servers, and there are other ways to pass information through a web link. One of the ways we've found includes having double-slashes. Microsoft Office XP now blocks those uses with no recourse.

Even if you accept the logic that double-slashes in hyperlinks are non-existent or bad, that doesn't change the more general principal that the user is entitled to type in something and have it stick, unchanged. If Microsoft wants to make a change for "cleanliness and consistency" they should build in a warning to the user and a way to reverse the change. A Smart Tag would work nicely. But in this case neither of these basic design courtesies is honored. The company has gone too far in compulsory changes to the link with no warning to the user or any workaround to fix the Autocorrect.

Adding injury to insult, there's no documentation on these changes in the help file. Microsoft has declined to provide details of any other compulsory changes made to hyperlinks in Office XP nor have they suggested any workaround for those affected, or some way to switch off this behavior. The Microsoft arrogance shows through: it's not a

problem, so  
why bother fixing it?

The fact that Microsoft has declined to detail what changes are arbitrarily made to links makes us even more concerned. Office XP users don't know what compulsory changes will be made to their links. Chances are they'll find out the way I did - the hard way.

Jonathan Arnold jdarnold@smartdrops.com Senior Product Developer  
Integrated Delivery Systems <http://www.smartdrops.com>

---

## Weatherbug

James Garrison <jhg@athensgroup.com>  
*Tue, 22 May 2001 17:31:03 -0500*

Someone recently sent me a reference to a program called Weatherbug and asked me to evaluate it from the perspective of a network admin for a small company where some employees are using it.

It's a Windows program that places a local temperature icon in your taskbar and then continuously monitors local weather data from the AWS Weathernet. If you click on the taskbar icon it displays a panel showing local weather data updated in near-real-time.

The service and Weatherbug executable are free and the whole thing is supported by advertising that is displayed in the Weatherbug window. I was curious about the security implications so I downloaded and

installed

Weatherbug with the intention of monitoring the IP traffic it generates with a packet sniffer.

The first thing that happens during install is you are asked if you want to also install two additional tools, "Gator" and "Offer Companion". Here's the blurb on the install dialog:

By including Gator and its OfferCompanion Software with Weatherbug, we're making your computer smarter!

Gator and OfferCompanion are among the web's most popular products. Gator fills in your passwords and online forms automatically - with no typing! And OfferCompanion delivers great offers to you based on web sites you visit!

The checkbox indicating that you want to install these "products" is checked by default. Needless to say, I did NOT allow it to install them (but then how do I know whether it listened to me or not ;-). Gator is clearly dangerous. I assume it keeps a database of previously seen web forms and the data you entered previously, and then re-enters the same data the next time you visit the same page. Regular RISKS readers should be cringing visibly by now :-)

Anyway, I started up Weatherbug and monitored its traffic:

- 1) During registration you are asked to provide quite a bit of personal info, including name, address, and income. Luckily (or I wouldn't have proceeded) all data is optional except for your Zip code, so it can locate weather stations nearby. The registration data is sent to a Weatherbug server in an HTTP GET request.
- 2) After you register, the software sends an HTTP POST to

216.33.111.107, which does not seem to have a reverse DNS entry. The POST data is:

```
InstallType=Full+Install&GatorStatus=Opt-Out&BCheck=
```

- 3) It appears to do everything over HTTP, so it's totally "pull" based. It does not *appear* to open any persistent connections. Also it seems to issue only GET requests in normal operation. I didn't see any POSTs other than the one described above. Of course, it's quite possible to send any data as parameters in a GET, so the absence of POST shouldn't be taken as implying anything positive.
- 4) In addition to retrieving weather data from the location you configured (any of over 5000 AWS sites located mainly at schools), it downloads ad gifs from doubleclick.net.
- 5) During registration you are assigned a registration ID that is sent to the Weatherbug server at various times. I did not see any evidence that the registration ID is sent to sites other than Weatherbug (i.e. ad requests didn't include the registration ID)
- 6) Every time Weatherbug starts up, my Win2K machine issues a single NETLOGON request to the PDC with a blank username, which is rejected. I don't know enough about MS authentication protocols to know if Weatherbug is doing this or it's just a byproduct of how Windows works.
- 7) When the main window is hidden (to a taskbar icon), most IP traffic stops. I still checks the weather data about once a minute but does not appear to load ads.
- 8) If you uninstall and re-install Weatherbug you are not asked to register again. The uninstall does not delete registry keys, so in order to completely remove it you must manually edit the registry.

I found no evidence that Weatherbug is "spyware", but then this

was a very cursory examination. It does seem to limit its data capture to your direct interactions with its GUI, but the possibilities for abuse are so high that I would not personally use it on an ongoing basis. It includes an automatic software update capability and there's no guarantee that future versions won't quietly slip in some "enhanced" data gathering techniques. When the capability is there, the temptation to use it has got to be tremendous.

Beyond the obvious security risks I'm also concerned about Weatherbug's bandwidth usage. When the main window is open and updating both weather data and ads in real time, it consumes about 20 kilobits/second. If you're a small company depending on an ISDN, DSL or fractional T1 link, it doesn't take very many of these to adversely affect other users.

I'm curious to know if anyone else has conducted a more thorough evaluation and analysis of Weatherbug.

James Garrison, Athens Group, Inc., 5608 Parkcrest Dr, Austin, TX 78731

jhg@athensgroup.com 1-512-345-0600 x150 <http://www.athensgroup.com>

---

## **★ 37% of programs used in business are pirated**

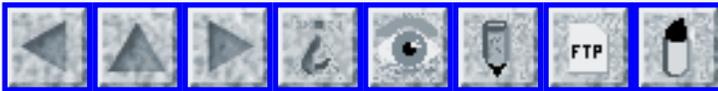
"NewsScan" <newsscan@newsscan.com>

*Mon, 21 May 2001 08:33:35 -0700*

Software piracy grew in 2000 for the first time in more than

five years,  
according to the Business Software Alliance, which estimates  
that 37% of all  
software programs used by businesses worldwide are illegal  
copies. The  
Asia-Pacific region -- where more than half of all software in  
use last year  
was stolen -- tops the list in terms of dollars (an estimated \$4  
billion)  
lost to piracy. Meanwhile, Eastern Europe has the highest  
piracy rate, with  
63% of its software illegally copied in 2000. In the U.S., 24%  
of programs  
are pirated copies. Although progress is being made in some  
regions, BSA  
director of enforcement Bob Kruger takes little comfort.  
"That's kind of  
like saying that I'm having fewer heart attacks than I used to.  
But the  
damage that's being caused by piracy is still devastating. It  
can be  
counted in the thousands of jobs and billions of dollars  
lost." (AP 21 May  
2001; NewsScan Daily, 21 May 2001;

<http://news.excite.com/news/ap/010521/07/software-piracy> ]



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 21: Issue 43

**Tuesday 29 May 2001**

## Contents

- [Xcel Energy wants to close Denver call center](#)  
[William Kucharski](#)
- [Topeka KS water treatment outage](#)  
[Jerry James](#)
- [WA public schools switching to risky new system?](#)  
[Phil Kos](#)
- [The World Bank meets on the Internet](#)  
[Andres Silva](#)
- [Eurocops want seven-year retention of all phone, Net traffic](#)  
[Hawkins Dale](#)
- [McDonald's testing cashless payments](#)  
[NewsScan](#)
- [Re: The Faith-Based Missile Defense](#)  
[Brian Clapper](#)
- [Re: Parnas's book on software](#)  
[John Graley](#)
- [Bugless = utopia](#)  
[Andrew Fleisher](#)
- [Another fear of Risks](#)  
[Bob Frankston](#)

- [Re: Word file turns into two disjoint texts](#)  
[Jeanne Sheldon](#)
  - [REVIEW: "Demystifying the IPsec Puzzle", Sheila Frankel](#)  
[Rob Slade](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

## ✶ Xcel Energy wants to close Denver call center

William Kucharski <kucharsk@mac.com>

Mon, 14 May 2001 03:53:11 -0600

According to the Rocky Mountain News, Xcel Energy, once Public Service of Colorado, wants to close their customer call center in Denver, meaning calls regarding service outages in Colorado would instead be routed to call centers in Minneapolis, MN, Eau Claire, WI and Amarillo, TX, with Xcel eventually wanting to consolidate all its call centers into one location.

The full story can be found at:

[http://www.rockymountainnews.com/drmn/business/article/0,1299,DRMN\\_4\\_453567,00.html](http://www.rockymountainnews.com/drmn/business/article/0,1299,DRMN_4_453567,00.html) [URL broken for readability]

Aside from the other obvious risks, given the problems Washington D.C. has with their 911 database ([comp.risks v.21.40](#)), I am not looking forward to how call centers several states away will react to a line being down or a natural gas leak in a rural or newly developed area which will likely not even exist on their maps.

Note that Xcel already serves twelve states with just the four call centers listed above...

William Kucharski <kucharsk@mac.com>

---

## **⚡ Topeka KS water treatment outage**

Jerry James <james@eecs.ku.edu>

*24 May 2001 12:45:03 -0500*

The *\*Lawrence Journal-World\** ([www.ljworld.com](http://www.ljworld.com)) reported on 22 May 2001 that Topeka (pop. ~122,000), the capitol city of Kansas, had suffered a water-treatment plant outage due to a power failure on Sunday. A storm passed through the area and knocked out power to some parts of the city, including the part containing the water-treatment plant. As a result, Topeka residents had to boil their water or buy bottled water, and drinking fountains across the city were turned off.

The article quotes a Lawrence official, who reassures residents of the smaller city (pop. ~80,000) that such an event is much less likely for Lawrence, since it has two water treatment plants on nearly opposite sides of the city.

---

## **⚡ WA public schools switching to risky new system?**

Phil Kos <PhilK@solthree.com>

*Wed, 23 May 2001 18:56:14 -0700*

An AP article dated 22 May that I read on aol.com

[http://my.aol.com/news/news\\_story.psp?type=1&cat=0100&id=0105220240181754](http://my.aol.com/news/news_story.psp?type=1&cat=0100&id=0105220240181754)

says that Washington state's public school IT cooperative (WSIPC, <<http://wsipc.org/>>) is spending \$20M on a new system from a company called Skyward (<<http://www.skyward.com/>>) that seems to raise more questions than it answers.

Among other things, student grades and attendance data will now be available on the Internet, and the system will supposedly also integrate such functions as administration, accounting, and scheduling. Some pretty specious comments are made regarding system security, e.g.:

"Skyward uses the same security measures that online retailers like Amazon.com use for credit card purchases over the Internet. The system also resists tampering because teachers continually revise the site."

Securing a system like this is theoretically possible, if the software itself is written well. But will security actually be implemented? Do the schools have people who are knowledgeable enough to administer the systems without leaving gaping security holes? I kinda doubt it. And if holes do pop up, the results could get pretty ugly. A lot of students will probably do their darnedest to hack the system. I expect that in most schools it won't turn out to be very hard, either by exploiting poor network configurations or just through basic social engineering, to find a back door.

The biggest problem I see with this change however is that it is

likely to become an attempt to replace a somewhat unwieldy but functional system (the current "old-technology" interface between parents and school officials) with one that has a totally different set of usage assumptions and failure modes, many of which will be confusing to anyone who wasn't involved in the production of the system. There's a strong possibility that schools adopting the new systems will try to switch over to using them exclusively, leaving technophobic--or just "unconnected"--parents out in the cold.

There's a logic error common in technological industries these days that says that a new technology will make any similar older technology obsolete, but this rarely works out the way the new tech evangelists think it will. In reality new technologies tend to co-exist with the old ones rather than replace them. (When I mentioned this error in response to yet another glowing futurist tech article predicting the death of CRTs, one of my colleagues here astutely replied "That's true, I heard it this morning on my radio.")

I sincerely hope that WSIPC gets things right here and this effort isn't a washout. \$20M is a fairly large wager when you're playing techno-craps. (Note that WSIPC headquarters is on Casino Road in Everett, WA... ;)

---

**🔥 The World Bank meets on the Internet**

Andres Silva <asilva@fi.upm.es>  
Mon, 28 May 2001 14:35:35 +0200

Having fear of anti-globalization activists, the World Bank announced the cancellation of its 2001 Annual Bank Conference on Development Economics (ABCDE) in Europe, originally slated to be held in Barcelona on 25-27 Jun 2001.

This is the WB news release on the subject:

<http://wbln0018.worldbank.org/EURVP/web.nsf/068c530cca07c3bac12569ed005af420/6b160161ef128660c1256a1e00541840?OpenDocument> [URL SPLIT]

As Barcelona streets seem dangerous, they are planning to move the conference to a "safest" place, as the internet (!). In the news release they say that "Fortunately the internet means that academic debates can now take place on line" and "plans are being made for an on-line discussion". OK. Let's see...

Andrés Silva <http://www.ls.fi.upm.es/UDIS/miembros/asilva>

[I thought about retitling this "The World Bank Meets The Internet", but thought better of it. PGN]

---

## 🔥 Eurocops want seven-year retention of all phone, Net traffic

"Hawkins Dale" <hawkins\_dale@watsonwyatt.com>  
Tue, 22 May 2001 17:44:06 -0700

Civil liberties publication Statewatch claims to have obtained leaked documents from the Council of the European Union (the 15 EU governments), which recommend the long-term retention of "every phone call, every mobile phone call, every fax, every e-mail, every website's contents, all internet usage, from anywhere, by everyone, to be recorded, archived and be accessible for at least seven years."

See <http://www.statewatch.org/soseurope.htm> .

It gets scarier!

The law enforcement agencies, argues the proposal, must have access to "user addresses, equipment identities, user name/passwords, port identities, mail addresses etc" The agencies are also to be provided with "the full name of the person (company), the residential address and credit card details."

Are they mad? One barely knows where to start enumerating the risks of such an undertaking.

Hawkins Dale [hawkins@REMOVEpobox.com](mailto:hawkins@REMOVEpobox.com)

---

## **⚡ McDonald's testing cashless payments**

"NewsScan" <[newsscan@newsscan.com](mailto:newsscan@newsscan.com)>

*Tue, 29 May 2001 08:43:31 -0700*

McDonald's Corporation has begun testing the use of a cashless

payment

system that uses the kind of radio transponder technology that was first developed by state highways to allow motorists to drive through toll plazas without having to stop to make a payment. McDonald's customers will wave the "Speedpass," a small transponder, at a drive-through window or at device inside the restaurant, and their transactions amounts will be immediately deducted from a "FreedomPay" account they've established on the phone or Internet backed by a major credit card. Similar systems have been used at Mobil gas stations and at some other fast-food restaurant chains. (Reuters/\*The New York Times\* 28 May 2001; NewsScan Daily, 29 May 2001

<http://www.nytimes.com/reuters/technology/tech-leisure-mcdonald.html>]

[To ensure that no one can forge the cards, I imagine they will use a BIG

MAC (that is, a long Message Authentication Code, perhaps also serving as

Mandatory Access Control). However, MACs tend to be much weaker than

cryptographic checksums security-wise. Of course, in the spirit of FAST

FOOD, if you are really in a hurry to pay for your meal with your

Speedpass and then ingest it rapidly, you might phone ahead on your car

phone to order your burger and fries in a liquid form: a BIG-MAC SHAKE,

with liquified meat, cheese, and bun (and perhaps including your cold

drink all in the same convenient take-out cup), which you could then wolf

down in one big gulp while driving and talking on your hands-free phone.

(I understand that vegetarians in some places already have a beef with

their fries. <Pun intended.>) But, given this new opportunity for ULTRA-FAST-FOOD, I think I'd rather FAST. After all, speed (with multiple meanings) can often lead to arrest (with multiple meanings). PGN]

---

## ✈ Re: The Faith-Based Missile Defense

Brian Clapper <bmc@WillsCreek.com>

*Thu, 24 May 2001 08:49:28 -0400*

Does anyone else find George W. Bush's global missile shield proposal eerily reminiscent of Reagan's Strategic Defense Initiative (a.k.a., "Star Wars")?

Here are some excerpts from a recent Bush speech (as transcribed on the Brookings Institution's web site [1]):

We must seek security based on more than the grim premise that we can destroy those who seek to destroy us. This is an important opportunity for the world to rethink the unthinkable and to find new ways to keep the peace. Today's world requires a new policy, a broad strategy of active nonproliferation, counter-proliferation and defenses. [...]

We also recognize the substantial advantages of intercepting missiles early in their flight, especially in the boost phase. The preliminary work has produced some promising options for advanced sensors and interceptors that may provide this capability. If based at sea

or on

aircraft, such approaches could provide limited but effective defenses.

We have more work to do to determine the final form the defenses might

take. We will explore all of these options further. We recognize the

technological difficulties we face, and we look forward to the challenge. Our nation will assign the best people to this critical

task. We will evaluate what works and what does not.

We know that some approaches will not work. We also know that we'll be

able to build on our successes. When ready and working with Congress,

we will deploy missile defenses to strengthen global security and stability.

For comparison, here's a quote from Reagan's March 23, 1983, speech, which

kicked off the SDI effort (as transcribed on the Federation of American Scientists web site [2]):

What if free people could live secure in the knowledge that their

security did not rest upon the threat of instant U.S. retaliation to

deter a Soviet attack, that we could intercept and destroy strategic

ballistic missiles before they reached our own soil or that of our allies?

I know this is a formidable, technical task, one that may not be

accomplished before the end of this century.

Yet, current technology has attained a level of sophistication where

it's reasonable for us to begin this effort. It will take years, probably decades of effort on many fronts. There will be failures and setbacks, just as there will be successes and breakthroughs. And as we proceed, we must remain constant in preserving the nuclear deterrent and maintaining a solid capability for flexible response. But isn't it worth every investment necessary to free the world from the threat of nuclear war? We know it is.

In the meantime, we will continue to pursue real reductions in nuclear arms, negotiating from a position of strength that can be ensured only by modernizing our strategic forces. At the same time, we must take steps to reduce the risk of a conventional military conflict escalating to nuclear war by improving our nonnuclear capabilities.

Surely, there are differences between the two initiatives, but it's the similarities that strike me.

The [very first issue of the Risks Forum Digest](#) contains a news item from

\*The New York Times\* announcing the resignation of David L. Parnas from an advisory panel on anti-missile defense. Parnas essentially asserted that the SDI would never work. [3]

Parnas' essays on the topic were ultimately collected and published in Communications of the ACM [4]. Here's an excerpt from Parnas' introduction to the CACM collection of essays:

The individual essays explain:

1. The fundamental technological differences between software engineering and other areas of engineering and why software is unreliable;
2. The properties of the proposed SDI software that make it unattainable;
3. Why the techniques commonly used to build military software are inadequate for this job;
4. The nature of research in software engineering, and why the improvements that it can effect will not be sufficient to allow construction of a truly reliable strategic defense system;
5. Why I do not expect research in artificial intelligence to help in building reliable military software;
6. Why I do not expect research in automatic programming to bring about the substantial improvements that are needed;
7. Why program verification (mathematical proofs of correctness) cannot give us a reliable strategic defense battle-management system;
8. Why military funding of research in software and other aspects of computing science is inefficient and ineffective.

Have we really made sufficient advances in software engineering-- in the way we build large systems, in reliability, in safety, in testability--so that this kind of project is more workable now than it was 18 years ago? Would David Parnas be less likely to resign from such an advisory panel today?

Perhaps my perspective is skewed from reading RISKS for 16 years, but I doubt we're substantially more prepared to build a such missile shield today than we were in the 1980s.

Brian Clapper, [bmc@WillsCreek.com](mailto:bmc@WillsCreek.com)

References:

[1] <http://www.brookingsinstitution.org/fp/projects/nmd/bush20010501.htm>

[2] <http://www.fas.org/spp/starwars/offdocs/rrspch.htm>

[3] The Risks Digest, Volume 1, Issue 1 (1 August 1985),  
<http://catless.ncl.ac.uk/Risks/1.01.html#subj6.1>

[4] Communications of the ACM, Volume 28, Issue 12 (December, 1985),

pp. 1326-1335. (ACM members can obtain a copy of this article through the ACM Digital Library.)

---

**Re: Parnas's book on software (Horning, [RISKS-21.42](#))**

John Graley <[jgraley@arm.com](mailto:jgraley@arm.com)>

*Tue, 29 May 2001 14:13:01 +0100*

A better experiment is to try it out and see if it works.

Without going into the highly debatable specifics, there's no doubt that we currently have a number of programming "paradigms" propagating around the software world purely or mainly because they are hard to argue with. I suspect other disciplines may be seeing this too.

Methodologies that are hard to argue with are likely to propagate though means such as: when people read books, when people study for qualifications, when they are trained by an employer, or when an employer instigates new procedures. OTOH, schemas that work in practice are typically

propagated  
through experimentation and shared experience.

That the former process is currently outpacing and outstripping the latter suggests that there remains something "unfocussed" about the way we approach methodology these days... maybe too much talking and not enough doing. That's a risk, for me anyway.

[In fact, Parnas \*has\* tried out many of these ideas in practice, for many years, with considerable success. PGN]

---

## ✶ Bugless = utopia

Andrew Fleisher <andrew8@start.com.au>

*Fri, 25 May 2001 13:48:49 +1000*

> In this case, I can't resist wondering how one can debug complex software  
> before deploying it. The danger is more in assuming one can and not  
> preparing for failure than in not doing complete debugging. This doesn't  
> mean one should not do any testing, just that the limits must be  
> recognized.

A source or corollary to the danger you cite is the expectation many people have that testing can prove there are no bugs. Testing can only prove there is/are bug/s.

> I'm a great admirer of MIR -- the ability to keep it going with just the  
> "chewing gum and bailing wire" (to use an old metaphor) impresses me more  
> than a design which is "perfect".

In my opinion, a practical person expects a 'perfect' design to include very easy repairability and maintainability. This is a significant source of risk reduction.

Andrew

---

## ✶ Another fear of Risks

"Bob Frankston" <rmf2gOther@bobf.Frankston.com>

*Wed, 23 May 2001 20:49:38 -0400*

I'm using IE 6.0 and it works pretty much like 5.0. With one notable exception -- UPS explicitly checks for it and doesn't let me use their service with an unapproved browser. I presume that feel it is better for them to lose customers than risk .. risk what?

I had a similar problem with IE 4=>5 with both UPS and Fleet. Fleet paid a price for this because they were totally unprepared for IE 5 when it shipped and it took a few days to fix their bugs.

UPS is loses two ways. They force me to use other services and they lose the value of users doing testing for them. They can warn me that they haven't tested with my browser but disallowing it is not only short-sighted, it represents a basic misunderstanding of the PC and the large effort put in to assure compatibility with previous versions of programs. Old MIS (before

they were called IT) departments did have a great fear of upgrades since each mainframe system was extensively patched. But that reasonable fear is now a phobia.

Bob Frankston <http://www.Frankston.com> <<http://www.frankston.com/>>

---

## ✶ Re: Word file turns into two disjoint texts (Page, [RISKS-21.40](#))

"Jeanne Sheldon" <jeannes@microsoft.com>

*Tue, 29 May 2001 08:39:15 -0700*

[This item is an out-of-band response to Clive that is included here with the permission of Jeanne Sheldon. It provides an interesting case history, especially with the Unicode wrinkle, and seems RISKS-worthy even if it may seem like an old problem. PGN]

Here's a summary of what I've been able determine about the document.

The document was created in Word 97.

Word was set to allow "Fast Saves", which is a non-default setting that performs incremental rather than complete saves. It is a feature intended to speed the save operation. More information on fast save can be found in Microsoft Knowledge Base articles:  
Q71999 WD97: "How to Disable the FastSave Option in Word for Windows"  
Q190733 WD97: "Opening Word Document in Text Editor Displays Deleted Text"(this was first documented in Q113052 CREATED: 23-MAR-1994)

Q192480 WD97: "Frequently Asked Questions About 'Allow Fast Saves'"

The document was saved three times; the second save was to a different filename. Because the second save initiates a second pass over the document, Word was able to compress the Unicode so that it was readable as ASCII characters and all incremental changes that were Fast Saved were collapsed. The first letter was then deleted and the letter to Dr. Page was composed. A single save was then performed to a local (non-network) drive using the same filename. Because "Fast Save" was enabled, the deleted text stream was identified but not actually deleted. Because a single save is a single pass and Unicode compression requires a second pass, the text remained as uncompressed Unicode. On Unicode compression, see: Q168967 "File Size Twice as Big When Compared to Earlier Version." While a non-Unicode aware tool would be unable to read the second set of text (the letter to you), it is actually quite readable on a Unicode-enabled text reader.

Extra notes: The document contains a unique identifier, indicating that the version it was authored on did not include the fix which removes that identifier. See Q222180 Unique Identifiers and Microsoft Office 97 Documents.

The document title, under properties, is generated automatically from the first line of the document on the first save. It is not subsequently updated, so it may contain text that is no longer in the document.

Comprehensive information on the topic:

Q223790 How to Minimize Metadata in Word Documents.

From Word 97online documentation:

The difference between a fast save and a full save

If you select the Allow fast saves check box on the Save tab in the Options dialog box (Tools menu), Word saves only the changes to a

document. This takes less time than a full save, in which Word saves the

complete, revised document. Select the Allow fast saves check box when

you are working on a very large document. However, a full save requires

less disk space than a fast save. If you are working on a document over

a network, clear the Allow fast saves check box. Fast saves cannot be

performed over a network.

You should do a full save in the following situations:

- \* Before you share a document with other people
- \* When you finish working on a document and save it for the last time
- \* Before you begin a task that uses a lot of memory, such as searching for text or compiling an index
- \* Before you transfer the document text to another program
- \* Before you convert the document to a different file format

Note: If you select the Always create backup copy check box on the Save

tab in the Options dialog box (Tools menu), Word clears the Allow fast

saves check box, because backup copies can be created only with full saves

... Clive, thank you very much for the time and effort that you have put

into this. Although the Word setting that caused the document to be

created in such a manner goes back to a time when electronic document

exchange was not the norm (and, over the past 7 years, much effort has gone in to attempting to assure that private information is not accidentally included) it is humbling and daunting to realize once again how difficult it is to correct the mistakes of past versions with software patches, bulletins and product documentation.

Jeanne Sheldon, Microsoft Corporation

---

## 🔥 REVIEW: "Demystifying the IPsec Puzzle", Sheila Frankel

Rob Slade <rslade@sprint.ca>

*Mon, 28 May 2001 15:58:15 -0800*

BKDMIPSP.RVW 20010511

"Demystifying the IPsec Puzzle", Sheila Frankel, 2001, 1-58053-079-6,

U\$75.00

%A Sheila Frankel sheila.frankel@nist.gov frankel@artechhouse.com

%C 685 Canton St., Norwood, MA 02062

%D 2001

%G 1-58053-079-6

%I Artech House/Horizon

%O U\$75.00 800-225-9977 fax: 617-769-6334 artech@artech-house.com

%P 273 p.

%T "Demystifying the IPsec Puzzle"

With its reference to the dim and distant past when Bill Gates was working on his fifth billion, the first sentence of the first chapter makes you suspect that this book will be a fun read. Which is a very strange thing to think about a security text. But the

readability

aspect becomes understandable when the author points out that this is not solely a work designed to turn out IPsec implementors (who may need additional references), but to inform purchasers and users.

IPsec is both a part of the "next generation" IPv6 standard, and a security option (or add-on) in the current IPv4. It is governed by some two dozen Internet RFCs (Request For Comments documents). While other security measures work only with specific programs, or at the transport layer, IPsec functions at the IP (Internet Protocol) or network layer, in order to address the widest range of applications and problems. It can address both confidentiality and authentication, as well as dealing with a number of denial of service (DoS) attacks that other security systems cannot.

Chapter one provides a general introduction, and a brief and apposite background of the Internet and IP layer functions. The author has culled a minimal foundation from the normal barrage of design and history, and even the description of IP headers is clear and important to the matter at hand. The Authentication Header (AH), which assures the detection of corruption or modification en route, is discussed in chapter two. The material also introduces basic structures such as the security association (SA) database, and provides some detail on implementation issues and concerns. The Encapsulating Security Payload (ESP) is described in chapter three, although not quite as lucidly as was the case for prior material. However, there is

also an excellent section outlining design considerations for the protocol.

Chapter four details the symmetric key algorithms used for AH and ESP operations, but does not go deeply into the asymmetric systems used by the Internet Key Exchange (IKE). IKE itself is discussed, in general in chapter five, with respect to remote users in chapter six, and listing additional options in chapter seven. The PF\_KEY application programming interface for IPsec is described in chapter eight. Chapter nine deals with issues of policy and policy enforcement. An overview of PKI (Public Key Infrastructure) is given in chapter ten. Chapter eleven looks at the special problems of multicast.

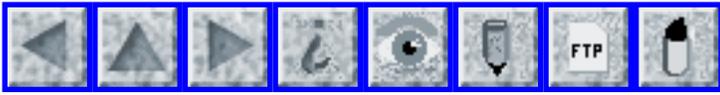
The book finishes off as many others start, with an analysis of whether IPsec can be the right solution to the problem.

The title of this tome is quite appropriate. It provides a clear outline and, if it isn't always articulate about the implications of portions of the system, it does a good enough job that the persistent reader will be able to work out other aspects. Not a book for the masses, perhaps, but for those who need either to purchase IPsec, or to choose between IPsec and other technologies, a very useful guide.

copyright Robert M. Slade, 2001    BKDMIPSP.RVW    20010511  
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 21: Issue 44**

**Monday 4 June 2001**

## Contents

- [House Science Committee hearings on voting systems](#)  
[Douglas W. Jones](#)
- [Swimming-pool changing cubicles](#)  
[Alan Barclay](#)
- [Insurer considers Microsoft NT high-risk](#)  
[Oleg Broymann](#)
- [UK Government Gateway blocks non-MS browsers](#)  
[Chatan Mistry](#)
- [The risks of clueless marketing](#)  
[Greg Searle](#)
- [Computer-generated mail -- too easy to fake?](#)  
[David G. Bell](#)
- [Forgery attempt -- risk of identity theft](#)  
[David Leshner](#)
- [Sex-offender database risks](#)  
[RISKS](#)
- [Crash leaves disabled riders stranded](#)  
[Jeremy Epstein](#)
- [BT upgrade: The best laid plans...](#)  
[John Sullivan](#)

- [Re: Software Engineering, Dijkstra, and Hippocrates](#)  
[Scot Wilcoxon](#)  
[Richard I Cook](#)
  - [Re: EU considers retaining \\*all\\* telecom traffic](#)  
[Michael Weiner](#)
  - [Re: NZ Electoral Web Site](#)  
[Richard A. O'Keefe](#)
  - [Re: Another Backhoe Reminder](#)  
[Arthur Marsh](#)
  - [Re: WeatherBug and Gator](#)  
[David Crooke](#)
  - [Re: 37% of programs used in business are pirated](#)  
[Jurek Kirakowski](#)  
[Merlyn Kline](#)
  - [More SMS SPAM](#)  
[Simon Waters](#)
  - [Re: Lost train](#)  
[Mark Brader](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

## ⚡ House Science Committee hearings on voting systems

"Douglas W. Jones" <jones@cs.uiowa.edu>  
*Tue, 29 May 2001 15:05:18 -0500 (CDT)*

On May 22, 2001, the House Committee on Science held a hearing entitled

"Improving Voting Technology: The Role of Standards", with Stephen Ansolabehere from MIT, Rebecca Mercuri from Bryn Mawr, Roy Saltman [retired from NIST], and myself -- Douglas Jones from the U of Iowa.

The House Science Committee web site has an archive of the written testimony submitted in advance of all committee hearings. For

this

hearing, they also have a real-audio webcast-transcript in their archive. See:

<http://www.house.gov/science/full/fchearings.htm>

It's sorted in reverse chronological order; scroll down to May 22, 2001.

In sum, I feel we presented a fairly strong united front on the key problems we face when using computers to count votes -- we agreed that current technology is poorly regulated, that many current voting systems have major defects, and that stronger standards must be put in place before any large-scale rush to replace "outmoded" voting systems with new technology.

We did disagree about whether a new standard would have an effect on the next presidential election. I was, I think, the most pessimistic in this regard. It may be that our answers depended on our interpretation of the question -- I assumed that it would take a year, at minimum, to put a new standard in place, and that it would take vendors a year, at minimum, to offer new machines based on this standard. I also assumed that old machines would be grandfathered in, so the new standard would not have a significant impact on real polling places for several more years as old machines were slowly phased out.

Doug Jones <jones@cs.uiowa.edu>

## **Swimming-pool changing cubicles**

Alan Barclay <gorilla@elaine.furryape.com>

*Mon, 28 May 2001 14:55:49 -0400*

\*The Register\* reports on French swimming pool "Centre Sportif Richard Bozon" at <http://www.theregister.co.uk/content/28/19236.html>. It seems that instead of a simple and traditional bolt on the doors to the changing cubicles, the centre has installed a computerized array of motion sensors, which detect if the cubicle is in use and displays a red or green light to indicate occupation. There is nothing to prevent someone from ignoring the lights and opening an occupied cubicle.

The obvious flaws are pointed out by \*The Register\*, including the problem for colour-blind people, and the sheer stupidity of putting in a high-tech solution to a low-tech problem, but they miss other problems, such as false positives and false negatives and the requirement to train the users of the facility of the meaning of the lights.

[Boz-on and Boz-off? Beau-saun(a)? Hose-sauna?  
But watch out for swimsuits with false positives. PGN]

---

## **Insurer considers Microsoft NT high-risk**

Oleg Broytmann <phd@phd.fep.ru>

*Tue, 29 May 2001 12:20:53 +0400 (MSD)*

[...] An insurance company has started to charge 5-15% more if you use Windows NT as a base for Internet services:

"We saw that our NT-based clients were having more downtime" due to

hacking, says John Wurzler, founder and CEO of the Michigan company, which

has been selling hacker insurance since 1998. Wurzler said the decision

to charge higher premiums was not mandated by the syndicates affiliated

with Lloyd's of London that underwrite the insurance he sells. Instead,

the move was based on findings from 400 security assessments that his firm

has done on small and midsize businesses over the past three years.

Wurzler found that system administrators working on open-source systems

tend to be better trained and stay with their employers longer than those

at firms using Windows software, where turnover can exceed 33 percent per

year. <http://www.zdnet.com/intweek/stories/news/0,4164,2766045,00.html>

Oleg Broytmann <http://phd.pp.ru/> phd@phd.pp.ru

---

## **UK Government Gateway blocks non-MS browsers**

"Chatan Mistry" <Chatan@iname.com>

*Mon, 28 May 2001 20:57:15 +0100*

An article appeared on *\*The Register\** on 28 May 2001. The original article

can be found at <http://www.theregister.co.uk/content/4/19239.html>

In short, the article briefly described an investigation by the UK Linuxuser magazine. It has found that the certificates being used on parts of gateway.gov.uk, the UK governments attempt at making all services available online by 2005, are specific to Windows and Internet Explorer 5.01. These signatures are currently provided by Equifax and ChamberSign. The article also goes to say that:

The Government Gateway doesn't exactly have much up on it at the moment, but the likelihood is that although simple registration by user name and password will give you access to some information services, all of the transactional ones will require use of certificates.

The one service available for individuals, electronic filing of tax returns, certainly does, so effectively only Windows/IE users can currently use it. UK.gov seems to have swallowed the Microsoft pitch whole; according to Linuxuser, the explanation given is that "other browsers do not give proper support for SSL and digital certificates."

I for one am very concerned. With Microsoft-based servers apparently being hacked almost at will, I can see a future when it will no longer just be the Internet where your identity can be used. And just for variety, what about if you are one of these people (aleit in the minority) that uses a non MS operating system or x86 hardware (such as a Mac)?

Of course, until the original Linuxuser article appears (the issue

containing this article goes on sale next week), not of this can be collaborated.

---

## **✶ The risks of clueless marketing**

"Greg Searle" <gsearle@s1.com>  
*Tue, 29 May 2001 11:22:58 -0400*

Has anyone else noticed the cluelessness of Microsoft's marketing when assigning a name to their new line of products? Do you think any of these marketing people are familiar with the popular "emoticons", or "smileys"? Has anybody else realized that "XP" is a person wincing and sticking their tongue out? Will the new MS products leave a bad taste in your mouth? :-b

[:-b is itself quite nice. A tongue-tied emoticon? PGN]

---

## **✶ Computer-generated mail -- too easy to fake?**

David G. Bell <dbell@zhochaka.demon.co.uk>  
*Sat, 02 Jun 2001 19:32:56 GMT +0000*

A front-page story in *\*The Yorkshire Post\** of 2 Jun 2001 reported that fake letters had been sent out in Bradford, requesting that people send \_original\_ birth certificates to enable the local council to recreate records lost through a computer error.

Original birth certificates are usable for identity theft.

The new twist comes from how the letters were created:

A council spokesman said they had no reason to believe council employees had stolen headed paper as the headings on most council correspondence were printed of on each individual letter by computer, and so could be copied by anyone who has received a letter by e-mail.

I'm not sure just what the computer-printed headings are, whether it includes some expensively-designed logo, and what details are actually included in e-mails. Obviously, it's that little bit easier to fake a letter if the genuine article is entirely computer-printed, rather than using old-fashioned pre-printed paper. Even with that barrier, people are becoming used to entirely computer-printed letters, headings and all.

I just hope I don't get an e-mail from Bradford council, if they have their logo attached as a graphics file.

[Original Yorkshire Post story by Amy Binns <amy.binns@ypn.co.uk>]

David G. Bell -- Farmer, SF Fan, Filker, and Punslinger.

---

## **✂️ Forgery Attempt -- risk of identity theft**

David Lesher <wb8foz@nrk.com>  
*Sat, 2 Jun 2001 11:11:06 -0400 (EDT)*

of a different sort....

<<http://washingtonpost.com/ac2/wp-dyn/A10385-2001Jun1?language=printer>>

... The package arrived bearing the official stamp of the Prince George's County clerk of the Circuit Court, the signature of the chief judge and a court order demanding the immediate release from prison of a triple murderer.

{details re: attempt to free prisoner with forged documents}

[Prince George's Chief Administrative Judge William D.] Missouri said he believes the signatures were photocopied from real court documents and pasted onto the fake release order. He suspects that someone inside the courthouse may have been involved. ...

This is not the first time copied signatures have been used. It won't be the last. But one wonders what the big push at retailers toward digitized credit-card slips will bring.

---

## **✶ Sex-offender database risks**

RISKS List Owner <risko@csl.sri.com>  
*Tue, 29 May 2001 16:02:19 -0500*

One of our readers was searching through the Illinois Registered Sex Offender database at

[http://samnet.isp.state.il.us/isps02/sex\\_offenders/index.asp](http://samnet.isp.state.il.us/isps02/sex_offenders/index.asp)

and ferreted out a wide variety of database errors, some of which could have really nasty consequences. There are lots of incorrect street addresses, ZIP codes, misspellings, inconsistencies, people living in different apartments shown with the same address, etc. The Chicago Police Department Sex Offender Database is not consistent with the Illinois State Police Sex Offender Information. To discourage vigilantes, the former database omits digits of addresses that are given in full in the latter, but the former has photos that are omitted by the latter. One wonders about how many entries point to the wrong person. Overall, the risks are many.

---

## ✶ Crash leaves disabled riders stranded

Jeremy Epstein <jepstein@acm.org>

*Sat, 02 Jun 2001 21:49:06 -0400*

MetroAccess is a Washington DC-area public transit system for the disabled (door-to-door service). Users call up at least 24 hours in advance to make a point-to-point reservation to get to/from work, shopping, medical care, etc. According to a 1 Jun 2001 article in *\*The Washington Post\** (<http://www.washingtonpost.com/wp-dyn/articles/A3679-2001May31.html>), Metro

Access lost all reservations for services due to crashes by both the primary and secondary systems. Those with regularly scheduled service (e.g., every day or every week) were recovered from a backup system, but

anyone with a one-time reservation was lost (about 1000 of the 2800 entries in the database).

The contractor that runs the system "has no idea who had placed the remaining 1000 reservations and made public pleas for anyone with a Metro Access reservation to call and confirm it." Which could, of course, lead to more failures as the system gets overloaded with calls.

The article claims that it was a hardware, not a software problem. No information was provided on how often backups are done, or how both the primary and secondary systems failed at once (seems quite unlikely if it truly is a hardware problem, unless both were hit by lightning or something like that).

---

## **✶ BT upgrade: The best laid plans ...**

John Sullivan <john@kanargh.force9.co.uk>

*Fri, 1 Jun 2001 19:02:50 +0100*

British Telecom currently offer two fixed-cost internet access plans for ISPs to resell. One ISP, PlusNet, has supported the old scheme (SurfTime) since last year. However they wanted to move over completely to the new scheme (FRIACO) which is simpler and cheaper. This has been in the pipeline for months. Amongst other differences SurfTime requires you to buy two separate components, one from the ISP and one from BT.

A couple of days ago an email was sent announcing today as the date of the big change. It recommended cancelling the BT component of SurfTime last night (the 31st May), as they would no longer be supporting at their end as of now.

Early this morning user accounts were migrated across, the FRIACO access numbers were enabled and the old SurfTime numbers were disabled. The problem is that both services require your local exchange to be upgraded and configured, by BT, just so. And many exchanges haven't been, resulting in many unhappy customers unable to dial in.

At 5pm (about 12 hours after the migration) PlusNet announced that the SurfTime access numbers had been re-enabled until such time as BT fixed their end of things. Unfortunately some people had already followed the instructions in their previous message to cancel their SurfTime subscription at the BT end last night...

One message from PlusNet reads:

> We are obviously very disappointed about this as we have spent months on  
> meticulous planning, but we have been let down somewhat by third parties.

Of course, with so much planning it was *\*bound\** to work first time. No need to keep the old service available until the new was *\*proven\** to work, oh no.

## **✶ Re: Software Engineering, Dijkstra, and Hippocrates (M.Cook, R-21.42)**

Scot Wilcoxon <scot@wilcoxon.org>

*Sun, 27 May 2001 10:55:37 -0500*

> The March 2001 issue of the \*Communications of the ACM\* contains an  
> article by Edsger Dijkstra called "The End of Computing Science?"

...

> As many of the RISKS entries have shown, application and other developers  
> have certainly made a mess of things at times, often of Laurel and Hardy  
> proportions ("That's another fine mess you've got us into."), and worse.

The title refers to "Computing Science". Most developers have never taken a Computer Science course, much less know the underlying concepts or apply them. I suspect many do not know who Dijkstra or the ACM are.

---

## **✶ Re: Software Engineering, Dijkstra, Hippocrates (M.Cook, [RISKS-21.42](#))**

"Richard I Cook" <ri-cook@uchicago.edu>

*Tue, 29 May 2001 12:03:46 -0500*

Michael Cook [no relation] wrote in [RISKS-21.42](#)

> If/when Software Engineering becomes a fully licensed profession, perhaps

> part of the code of ethics should be similar to the intent of  
> part of the  
> Hippocratic Oath, "First, do no harm". This is a paraphrase  
> of the  
> statement "The health and life of my patient will be my first  
> consideration" which is from the World Medical Association's  
> "Declaration  
> of Geneva" of 1948.

Speaking from experience as a member of the profession for which  
that oath  
was originally developed, I would suggest that Michael's  
laudable objectives  
might better be pursued via some other route.

Richard I. Cook, MD

---

## **✶ Re: EU considers retaining \*all\* telecom traffic (Weingart, R-21.42)**

"Michael Weiner" <michael\_weiner@gmx.net>

*Mon, 28 May 2001 08:17:35 +0200*

Dave Weingart reported on EU plans to retain all telecoms  
traffic.

Apparently, the EU is not that ambitious, but the issue is  
critical enough.

Current EC telecommunications law protects the privacy of  
telephone users by

obliging the operator to delete or anonymize traffic data as  
soon as there

is no more pressing need to retain it (e.g., as the bill for the  
services

have been paid, etc. - see article 6 of

[http://europa.eu.int/eur-lex/en/lif/dat/1997/en\\_397L0066.html](http://europa.eu.int/eur-lex/en/lif/dat/1997/en_397L0066.html)).

Law enforcement agencies find this cumbersome as it does not  
allow them to

obtain information on past telephone usage (for the period before they placed a tap). Statewatch, a British NGO active in the field of privacy protection, has published a leaked EU Council document on its website that urges the Commission "to review [...] the provisions that oblige operators to erase traffic data or to make them anonymous" in order to "ensure that the purpose limitations regarding the personal data do not come into conflict with the law enforcement authorities' needs of data for crime investigation purposes":

<http://www.statewatch.org/news/2001/may/enfo7277.htm>

If this initiative is acted upon, it will significantly reduce the privacy protection of telephone users in the European Union. Network operators will have to foot the bill for providing the necessary storage space and for carrying out the database searches that will no doubt be requested by law enforcement agencies.

---

## ✉ Re: NZ Electoral Web Site

"Dr Richard A. O'Keefe" <ok@atlas.otago.ac.nz>  
*Fri, 25 May 2001 14:39:53 +1200*

I've had some responses to my note in [RISKS-21.41](#). Others have confirmed that they find the pages unreadable. The site maintainer has also been in contact, and in fairness I think I should make these points.

- (1) NZ law requires a signature on any application to change electoral roll records; what the Web site does is let you fill out a form electronically which you can then fill in, sign, and post, or you can ask them to print the completed form and post it to you.
- (2) This means that the newspaper report that you can enroll and change your record ONLINE is at best a half-truth. RISK of believing the newspapers?
- (3) The maintainer did not respond with an angry defence but has sought constructive advice about improving the site. I sent some advice, and was given a thank-you.
- (4) It's more secure than I said. Apparently, had I been able to get further, I would have been asked for my house number as well. (No comment on my part required.)
- (5) I was assured that the site had been "extensively tested": on Windows, using Netscape 4 and IE 4. They don't apparently have a Mac to test things on.
- (6) The fact that I can't get through \*may\* have something to do with the support (or lack of it) for SSL at this end. (iCab indicates this with "Network error #-15", some browsers are better, some are even worse.)

There remains the Risk of a NZ Government project being placed in a position where "extensive testing" has to mean Windows-only.

---

## ✶ Re: Another Backhoe Reminder (Felsche, [RISKS-21.41](#))

Arthur Marsh <arthur.marsh@adelaide.edu.au>

Thu, 24 May 2001 16:06:19 +0930

I doubted that there were "thousands" of fibres to reconnect, and looked

for other accounts of the incident. ZDNet Australia had an account at:

<http://www.zdnet.com.au/news/dailynews/story/0,2000013063,20222584-1,00.htm>

that included:

Telstra crews had to replace 1.5 kilometres of cable and reconnect

every individual fibre optic wire within it - about 150 strands in total.

Arthur Marsh, Network Support Officer, Information Technology Services

The University of Adelaide SA 5005 Australia Ph: +61 8 8303 6109

[PGN notes: This was also discussed by Kent Borg, who added a Lesson: Just because someone is an official spokesman doesn't mean he

actually knows what he is talking about. Also, just because something

is written with quote marks doesn't mean the quote is accurate.

Someone clearly confused the image of a trunk of a zillion copper

pairs with fiber optic cables and came up with a mule that doesn't

exist; and no Australian Broadcasting Corporation editor caught it.]

---

## ✶ Re: WeatherBug and Gator (Garrison, [RISKS-21.42](#))

David Crooke <dave@convio.com>

Sat, 26 May 2001 00:37:27 -0500

Your correspondent seems surprised that the accompanying Gator product

offers to store passwords, but this is a feature of more than one modern

browser (Mozilla and Internet Explorer spring to mind) and of almost every

one of Microsoft's own products, including (laughably but sadly) their PPTP

VPN client.

**⚡ Re: 37% of programs used in business are pirated ([RISKS-21.42](#))**

jk <jzk@ucc.ie>

Mon, 28 May 2001 13:49:58 +0100

This study clearly has shock value as it combines seemingly objective data and emotive language. I have noted a number of misquotations of its findings in various news announcements and tried to find out how this figure of 37% is really computed.

But first of all, as to credibility of source: does the Business Software Alliance (BSA) have any vested interest in artificially inflating or deflating this figure? The International Planning and Research (IPR) organisation which seems to have advised the BSA says that 'BSA educates computer users on software copyrights; advocates public policy that fosters innovation and expands trade opportunities; and fights software piracy.'

The BSA report at <http://www.bsa.org/resources/2001-05-21.55.pdf> concludes that 'To ensure a high level of confidence, member companies of BSA reviewed the results of the study and their input was used to validate and refine the study assumptions'.

This sounds like an inherently highly risky procedure for obtaining the truth. But to press on...

The methodology, from what I can understand of it, compares the number of

computers sold to each country with the amount of software sold to that country (lots of various 'adjustments' for replacements, maturity etc the bases of which are not explained). The number of computers sold is then multiplied by a number (again, all highly convoluted, but no hard details as to where these magic numbers come from) to give a figure for the demand for software given the hardware sales. The difference between this figure and the amount of software actually sold is the amount of 'piracy'. This is in fact a gross simplification of their actual methodology but seems to be the essence of it. It relies a lot on magic numbers.

In comparison to the coyness of the description of how all the magic numbers are computed, the final data, \*is\* displayed in glorious detail per country, per year, dollar loss, etc.

If the way the magic numbers were arrived at is fair and above board, then it would make sense to publish details of the process in order to boost the confidence of the report and to show that not only does it make an emotive point, but that it has good grounds for doing so. Otherwise, given the source, one may be tempted to dismiss it on the grounds of possible self-interest by the authors (if they wish to fight software piracy, they could hardly publish a report which says that software piracy doesn't exist, could they?)

I spoke last summer to a technical manager of a medium-sized company in one of the so-called 'black spots' of software piracy fingered in

the report.

He told me that when they up-sized, the company had moved from MS Office to Star Office, because the latter was being given away for free. He also told me of how the company sourced shareware and freeware because he didn't trust 'black-market stuff'. Shareware is usually an order of magnitude cheaper than commercial stuff, and you often get to keep in touch with the folk that created it as well. He and I have remained in contact and swapped some interesting resources, so it isn't all talk.

His approach sounded eminently rational to me: if you're poor, buy the hardware and find free- and share-ware on the web. All of a sudden, the conclusions of BSA report sounded a lot more risky to me.

Jurek Kirakowski, HFRG, Ireland <http://hfrg.ucc.ie/> <http://hfrg.ucc.ie/jk/>

---

## **★ Re: 37% of programs used in business are pirated ([RISKS-21.42](#))**

"Merlyn Kline" <merlyn@zynet.net>

*Tue, 29 May 2001 16:25:51 +0100*

> tops the list in terms of dollars (an estimated \$4 billion) lost to piracy.

This sounds like one of those inflammatory and inflationary statements the RIAA has become fond of recently. To my mind there is a big difference between this statement (which describes something that I can't imagine a

means of estimating) and a statement like "tops the list in terms of dollars (an estimated \$4 billion) retail value of pirated software". Many users would not be using the software they are using if they were forced to buy it rather than pirate it - they would be using a cheaper alternative.

---

## ✉ **More SMS SPAM (Re: Moskowitz, [RISKS-21.42](#))**

Simon Waters <Simon@wretched.demon.co.uk>  
*Sat, 26 May 2001 19:58:02 +0100*

Robert Moskowitz's Risks article 'Great DoS attack for cell phones' prompted me to write.

This week I've received two identical SMS messages telling me to urgently call a number, normal enough for a busy IT consultant perhaps, but the number was for a premium rate line.

Such abuses are not specifically SMS related (A favourite UK scam was to make very cheap goods and holiday offers via junk fax, where to accept it the order must be sent to a premium rate fax number - no doubt some Office employees figured they would turn their employers phone bill into their holiday money and ordered despite knowing the number was premium rate), although the ever changing number schemes inflicted on the average Brit by our telecoms regulator is making it harder and harder to sort out the wheat

from the chaff, and the sheer number of mobile phones will make these scams more profitable and presumably therefore more common.

At least I may have found a use for the premium rate number blocking service offered by many mobile phone operators, it will let people act on their SMS messages without be lumbered with an unexpectedly large bill.

Perhaps someone would care to enlighten me as to what urgent messages I declined to pay for?

Simon Waters [www.eighth-layer.com](http://www.eighth-layer.com) Tel: +44(0)1395 232769 ICQ: 116952768

Moderated discussion of teleworking issues at [news:uk.business.telework](mailto:news:uk.business.telework)

---

## **Re: Lost train (Weber-Wulff, [RISKS-21.42](#))**

Mark Brader <[msb@vex.net](mailto:msb@vex.net)>

*Wed, 30 May 2001 11:45:01 -0400 (EDT)*

I don't think the Swiss Federal Railways (Schweizerische Bundesbahnen, SBB, <http://www.sbb.ch>) could have been involved here: the lines from Chur to Davos are part of the Rhaetian Railway system (Rhaetische Bahn, RhB, <http://www.rhb.ch>).

Mark Brader, Toronto, [msb@vex.net](mailto:msb@vex.net)

[Correction noted in [RISKS-21.43](#). But could be a joint arrangement? 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 21: Issue 45**

**Wednesday 6 June 2001**

## Contents

- [Ed Felten and researchers sue RIAA, DoJ over right to publish](#)  
[Declan McCullagh](#)
- [Billboard error message](#)  
[Phil Agre](#)
- [California bill prohibits online gambling](#)  
[Jim Griffith](#)
- [Dutch government to act against virtual child pornography](#)  
[Marcus de Geus](#)
- [Payday delayed by one day in Belgium](#)  
[Kris Carlier](#)
- [Mobile phones to manage truancy - and other free publicity](#)  
[Nick Brown](#)
- [Inevitability of risks](#)  
[Mick Topping](#)
- [Re: The Faith-Based Missile Defense](#)  
[S. Alexander Jacobson](#)
- [Re: Eurocops want seven-year retention of all phone, Net traffic](#)  
[Morten Norman](#)
- [Re: Our software is \\*never\\* wrong](#)  
[Scott E. Preece](#)

- [WSJ/Word change tracking/"MS Tool Lifts Veil on Spin"](#)  
[Daniel P. B. Smith](#)
  - [Re: Word file turns into two disjoint texts](#)  
[Lloyd Wood](#)
  - [Steve Gibson: Windows XP Vulnerable; Big ISPs just don't care](#)  
[Chris Meadows](#)
  - [Re: Office XP modifies what you type](#)  
[Bear Giles](#)  
[LShaping](#)
  - [Re: "Hacker Insurance" charges higher rates for Windows systems!](#)  
[Elana](#)
  - [Re: UK Government Gateway blocks non-MS browsers](#)  
[David G. Bell](#)
  - [10th USENIX Security Symposium](#)  
[Tiffany Peoples](#)
  - [Announcement - 16th Annual Software Engineering Symposium 2001](#)  
[Carol Biesecker](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

## ✶ FC: Ed Felten and researchers sue RIAA, DoJ over right to publish

Declan McCullagh <declan@well.com>

Wed, 06 Jun 2001 10:01:08 -0400

Code-Breakers Go to Court

By Declan McCullagh (declan@wired.com), 6:22 a.m. June 6, 2001  
PDT

WASHINGTON -- After a team of academics who broke a music-watermarking scheme bowed to legal threats from the recording industry and chose not to publish their research in April, they vowed to "fight another day, in another way."

On Wednesday, Ed Felten of Princeton University and seven other researchers took their fight to a New Jersey federal court in a lawsuit asking that they be permitted to disclose their work at a security conference this summer.

Joining them is the Usenix Association, a 26-year-old professional organization that has accepted Felten's paper for its 10th security symposium in Washington during the week of Aug. 13. The Electronic Frontier Foundation is representing the researchers and Usenix.

In what appears to be the first legal challenge to the Digital Millennium Copyright Act's criminal sections, Usenix is asking the court to block the Justice Department from prosecuting the conference organizers for allowing the paper to be presented. [...]

[<http://www.wired.com/news/mp3/0,1285,44344,00.html>]

Background:

<http://www.politechbot.com/cgi-bin/politech.cgi?name=felten>

DMCA-related photos:

<http://www.mccullagh.org/theme/dmca-appeals-arguments.html>

<http://www.mccullagh.org/theme/dvd-2600-trial.html>

<http://www.mccullagh.org/theme/dmca-protest.html>

EFF document archive:

[http://www.eff.org/Legal/Cases/Felten\\_v\\_RIAA/](http://www.eff.org/Legal/Cases/Felten_v_RIAA/)

POLITECH -- Declan McCullagh's politics and technology mailing list

You may redistribute this message freely if you include this notice.

To subscribe, visit <http://www.politechbot.com/info/subscribe.html>

This message is archived at <http://www.politechbot.com/>

---

## ✶ Billboard error message

Phil Agre <pagre@alpha.oac.ucla.edu>

*Mon, 4 Jun 2001 19:10:09 -0700*

I was driving on I-405 northbound in southern Los Angeles County when I saw a bitmapped billboard on the east side of the road that was displaying a Windows error message. I couldn't take down the exact text, but it was something like "The file cannot be played; it may be corrupt". This was a first for me. I had seen Windows error messages displayed on video monitors in airports and other public places, but never on a full-sized billboard. Now, digital billboards that display animation are already a Risk of distraction to passing drivers; there is an especially bright billboard on the Sunset Strip that is IMHO a serious traffic hazard, and it often plays music videos and the like. I don't know what the billboard on I-405 normally shows. One might argue that the giant Windows error is actually an anti-Risk because it reminds the entire populace just how unreliable Microsoft products are, thus reducing the likelihood that a passing motorist will specify such products as part of a safety-critical system once they get to work. On the other hand, it is easy to imagine the havoc that could be caused by someone who managed to hack a billboard next to the freeway and display their own content on it, particularly if the billboard

is supposed  
to display safety-relevant traffic messages.

Phil Agre

[Phil, Please drive safely, with hands-free cell phone headset (unless you already have a dashboard-mounted videocam/videophone set), coffee in one hand, a hot dog in the other, while watching your GSP video screen at the same time. Then you can safely ignore the safety-related signs.

BTW, My local movie N-plex recently displayed a bunch of operating system prompts and reboot script in the space devoted to which shows were sold out. We've also had reports of similar activities in RISKS.  
PGN]

---

## **California bill prohibits online gambling**

<griffith@olagrande.net>

Wed, 30 May 2001 18:43:08 -0500 (CDT)

The California Assembly passed a bill today which would make it illegal for Californians to play games online that are otherwise illegal in California. The bill would fine first-time transgressors \$25 per transaction (not conviction) and \$100 per transaction thereafter. Companies (anywhere) convicted of catering to Californians could be liable for \$1000 per transaction and 90 days in jail. The bill supposedly

specifically allows  
prosecutors to go after offshore corporations.

<http://www0.mercurycenter.com/breaking/docs/064216.htm>

We're barely finished cursing France for their stupidity in  
attacking  
Yahoo!, and we go and do something equally stupid. Hopefully,  
our Senate or  
Governor is a little smarter than our Assembly.

Anyone want to bet that this bill doesn't work as intended? No,  
wait a  
minute, I could get arrested for that.

---

## 🔥 Dutch government to act against virtual child pornography

"Marcus de Geus" <marcus@degeus.com>

*Thu, 31 May 2001 09:38:35 +0000*

The Dutch Minister of Justice, Korthals, has announced measures  
that will  
make it illegal to produce or possess child pornography created  
by means of  
electronic image manipulation. The proposed legislation appears  
to be aimed  
at preventing the production and possession of artificially  
rendered images  
that could be interpreted as representations of children  
involved in sexual  
acts. Current Dutch law states that the production or possession  
of  
pornography is a criminal offence if it involves the physical  
(ab)use of  
(real) persons under a certain age. [Based on a report in an e-  
mail message  
from Radio Nederland Wereldomroep.]

Leaving aside for the moment the moral issues involved, as well as the practical aspects of enforcement, or even the difficulty of ascertaining the age of a virtual person, the legal ramifications could prove interesting, since the proposal appears to be based on the assumption that the virtual representation of an activity can somehow be put on a par with its physical counterpart.

Few, if any, people will be prepared to argue in favour of sexual acts involving children, which is why it is an illegal activity. In the same vein, few would argue in favour of the wholesale slaughter of people for the purpose of entertainment. We find the idea repugnant, which is why such activities have also been made illegal, at least in most modern countries.

On the basis of these premises, I wonder how the widespread legal availability of virtual reality shoot-'em-up computer games will affect, or be affected by, the proposed legislation. I somehow doubt that Mr. Korthals will be prepared to do battle with such economic forces as represented by Messrs. Sony, Nintendo, and soon, Xbox producers, Microsoft.

The RISKS? Assuming that seeing is believing, or that What You See Is What You Get.

Marcus de Geus <marcus@degeus.com> <http://www.degeus.com>

---

**✈ Payday delayed by one day in Belgium**

Kris Carlier <root@iguana.be>

Sat, 2 Jun 2001 10:38:44 +0200 (MET DST)

On 1 Jun 2001, the majority of people on the government payroll were paid with a one-day delay. The same goes for refunds for VAT and taxes. The reason: Belgian postal services are tasked with doing the money transfers towards the different banks.

Seems that they had a special situation: on 31 May, not only people had to be paid, but the next weekend (02-04 Jun) being a long one, an 'exceptionally large number' of transactions were fed to the system. In itself this should not have been a problem, but the system has some built-in time-restrictions, described as being rather 'large'. This of course to avoid runaway jobs from causing further damage, just in case. Yet, some components were hitting these time-restrictions before they were actually finished. The Post's spokesman said that this kind of situation is only encountered once in 5 years.

At first, of course, the functionaries were suspecting their respective payment departments to be responsible. Phones didn't stop ringing all day, then finally it was also on the news.

kris carlier - kris@iguana.be KC62-RIPE SMS: +32-475-61.43.05

---

**🔥 Mobile phones to manage truancy - and other free publicity**

BROWN Nick <Nick.BROWN@coe.int>

*Fri, 1 Jun 2001 16:11:51 +0200*

\*The Guardian\* (UK) "reports" (by printing a press release) today on a "system" to allow teachers to report truanting children to their parents.

The "article" contains a number of less-than-stunning revelations, such as that "a large number of parents have mobile phones", and some highly meaningless claims, for example "The device can also be used to inform headteachers, therefore cutting down on the time the overall monitoring process takes."

Full text:

<http://www.guardian.co.uk/Archive/Article/0,4273,4196245,00.html>

(and don't forget to click on the related story at the end, about students calling their parents from the classroom to complain about their teachers !)

The RISKS should be fairly obvious to regular readers, both in the system itself, and also in the phenomenon of supposedly "upmarket" newspapers with a tradition of investigative reporting, printing technology company press releases as news. A further example of the latter is the collection of unverifiable claims in the "article" on Microsoft Office XP at <http://www.guardian.co.uk/Archive/Article/0,4273,4196242,00.html>.

Nick Brown, Strasbourg, France

---

**✶ Inevitability of risks**

"Mick Topping" <mick@mtopping.com>

Fri, 1 Jun 2001 22:27:15 -0500

Apparently the Gullibility Virus

<http://bob.bob.bofh.org/~robm/manual/virus/gullibility.html>

has struck more people than first realized

Remember this from several months back?

Subject: New Minnysoota Virus.

Sven and Ole vere here.

Yew have yust received da Sven & Ole Computer Virus.

Because ve don't know how to program computers, dis virus verks

on da honor system. Please delete all da files on yewr hard drive

manually and forward dis message to everyvon on yewr mailing list.

Tank yew fer yewr kewhopeeration.

Sven and Ole

I thought this was pretty funny, at the time, but then I saw the recent

warnings on the Hoax-Virus, like this:

<http://www.thestandard.com/article/0,1902,26780,00.html> It

suddenly came to

me, that someone had taken the Sven&Ole model, and improved on it, just a

little. AND IT IS WORKING! Apparently you don't even have to be a

script-kiddy to make an effective virus. (Hey kid, if you put sugar in your

dad's car's gas tank, it will run real fast...Well, Joe, if you want to get

that charcoal started FAST, try this jar of gasoline...If you don't have a

fuse, just stick a penny in the socket...memes?) It is not

surprising that a few users might fall for this, but the very fact that something like this can find a toe-hold to spread, confirms that a big risk of technology (ignorance) has been with us since the first tool user cut himself with the first sharp rock.

Is real risk of information technology is that it enables the ultra-rapid spread of malicious memes?

---

## ✶ Re: The Faith-Based Missile Defense

"S. Alexander Jacobson" <alex@shop.com>

*Tue, 29 May 2001 20:49:06 -0400 (Eastern Daylight Time)*

I find it surprising that people on this list are so dismissive of anti-ballistic missile technology:

- \* the US and Russia both use and sell various forms of surface to air missiles designed to shoot down even very fast planes like F-16s and MIG-29s.

- \* attack missiles in terminal phase seems like a natural extension of the capabilities of existing SAM systems (not a radically new technological development)

- \* missiles in boost phase are very hot and move very slowly and predictably (much more so than highly maneuverable fighter planes) -- so there is some reason to believe that boost phase systems can be more effective

than SAMs.

From a technical perspective, development of boost phase interception does not seem obviously more complex than that of Aegis ship based defense system.

Moreover, general ABM seems like a natural extension of the Aegis system in particular. We now know that the USSR actually deployed an integrated missile tracking system at Krasnoyarsk -- so at very least that portion of the technology is actually deployable.

Obviously developing and deploying ABM systems will not be easy and there is substantial risk of failure. Moreover even a successful project will may be substantially less than 100% effective. However, the same is true of most defense systems, but we develop and deploy them anyway. Why hold ABM to a different standard than other defense technology?

Critics may have good policy reasons to oppose deployment of ABM systems, but creating FUD about development risks is a service to no one.

Alex S. Alexander Jacobson 1-646-638-2300

---

## **⚡ Re: Eurocops want seven-year retention of all phone, Net traffic**

<marten-risks@norman.qmail.com>

*Tue, 5 Jun 2001 21:58:39 +0200 (MET DST)*

> Are they mad? One barely knows where to start enumerating the risks

> of such an undertaking.

Try to remind the politicians of snail mail and the fact that anyone may send a letter anonymously by dropping it in a mailbox.

I humbly suggests them to put a clerk and a photo copy machine at every snail mail box. Let the clerk identify everyone droppping a letter. And of course open the envelope and make a photocopy of the letter to be archived for seven years.

If they still think it's a good idea, vote for other politicians.

Morten Norman

---

## ✉ **Re: Our software is \*never\* wrong (Gat, [RISKS-21.41](#))**

"Scott E. Preece" <preece@urbana.css.mot.com>  
*Thu, 31 May 2001 14:59:40 -0500 (CDT)*

It is possible to explain this without the credit-card company rep being either stupid or over-trusting. If the database tracks changes to the data and the rep was aware of an automated change (a systematic change to the database, such as might occur in changing the schema in the database), the rep might be able to know that you should have gotten a preference update notification and that no manual changes had been made to your data.

Obviously, it is also possible that there was some break-in, but if the rep had a reasonable explanation consistent with all the data, Occam's razor

argues for assuming that explanation.

scott preece, motorola/css urbana design center preece@urbana.  
css.mot.com  
1800 s. oak st., champaign, il 61820 1-217-384-8589

---

## ✶WSJ/Word change tracking/"MS Tool Lifts Veil on Spin"

"Daniel P. B. Smith" <dpbsmith@bellatlantic.net>

Wed, 30 May 2001 20:01:22 -0400

If you send a Word .doc file directly to someone else, without going to "track changes" and accepting all changes, your recipient can see all the edits you have made to the document, with results that can be humorous, embarrassing, or worse. This is old news to RISKS readers--how long ago did the first mention of the problem appear in RISKS? But perhaps the recent appearance of an article about it in The Wall Street Journal (May 14th, page C1) is worthy of mention.

The article is entitled "How to Read Between the Corporate Lines." It gives the procedure for viewing Microsoft Word edits, and (with somewhat less clarity) the procedure you must go through to prevent someone else from viewing YOUR edits.

The way the Journal puts it: "Just a couple of clicks provides a revealing peek into how some companies massage their public messages to Wall Street." In a news release from Ameritrade Holding Corp, "in one draft, Ameritrade billed the March hiring of Mr. Moglia as one of the 'right decisions' the company made during a difficult second

quarter.

But his name ended up on the cutting-room floor, a thin blue line erasing him from the final version." It mentions that "Analysts and investors looking at an earlier draft would have found a per-share, quarterly loss of 31 cents. But that, too, was crossed out and change to a loss of 30 cents." An Ameritrade spokeswoman brushed off the changes, saying "it is too bad--but on the other side of it, it is too bad that someone would think to turn the edits on."

The article goes on to cite minor gaffes from Visa USA, Allied Capital, Web Street, and Acxiom, leaving little doubt that the problem is widespread.

There are no real howlers or scandals here. But you'd think the RISKS would be obvious, wouldn't you?

Daniel P. B. Smith <dpbsmith@world.std.com>  
"Lifetime forwarding" address: dpbsmith@alum.mit.edu

---

## **⚡ Re: Word file turns into two disjoint texts (Page, [RISKS-21.40](#))**

Lloyd Wood <l.wood@eim.surrey.ac.uk>  
*Wed, 30 May 2001 20:05:28 +0100 (BST)*

> Word was set to allow "Fast Saves", which is a non-default setting  
> that performs incremental rather than complete saves.

It's worth pointing out that for a long time the default was to have fast save on. The first thing I would do with any version of

Word is

check for and disable it, having discovered its lack of reliability.

(Many patches to earlier versions of Word were solely to address, er, issues with fast save.)

The risk lies in changing the defaults when user experience has led to certain expectations. In this case, if you were hoping that fast save would let you recover mistakenly deleted text based on experience of older versions of Word, you'd be out of luck.

<L.Wood@surrey.ac.uk>PGP<<http://www.ee.surrey.ac.uk/Personal/L.Wood/>>

---

## ★ Steve Gibson: Windows XP Vulnerable; Big ISPs just don't care

Chris Meadows <robotech@eyrie.org>

*Mon, 04 Jun 2001 22:57:10 -0500*

The report on this webpage

<http://grc.com/dos/grcdos.htm>

is from Steve Gibson, a respected name in the tech community, and it details his travails after grc.com came under attack from a 13-year-old hacker, at first due to a mistaken belief Gibson had called him a name, then simply because it was fun. It mentions how Windows XP was all but made with these so-called "script kiddies" in mind, and they're aware of it--and when it is more widely spread, they will be able to launch

devastating, perhaps unstoppable attacks.

He also mentions how much trouble he had getting any of the major ISPs to cooperate with him.

This is an eye-opening report. Ignore it at your peril.

Chris Meadows aka Robotech\_Master Co-moderator rec.toys.transformers.moderated  
robotech@eyrie.org <URL:<http://www.eyrie.org/~robotech/>>

---

## ✂ Re: Office XP modifies what you type ([RISKS-21.42](#))

Bear Giles <bear@coyotesong.com>  
*Tue, 29 May 2001 23:42:20 -0600 (MDT)*

I believe that the RISKS here are far more profound than a few broken links.

In the beginning, authors were responsible for their own words and our programs (confusingly called 'editors') preserved them. Until those butchers, our human editors, hacked at them.

Then computers became powerful enough for 'editors' to act as advising editors. We still owned our own words, at least until they-who-edit-because-they-cannot-write got ahold of them, but the programs could handle the tedious work of digging out the dictionary.

Now, for the first time, we see a program usurping the role of the human editor. Unlike the human counterpart, we can't bribe this one with cheap booze when the facts fail to sway them. On this issue the

program is the  
FINAL editor, sans appeal.

This is... scary. The smaller problem is one of liability - if a human editor screws up, he can face real consequences. But if a program is responsible for dropping a single word from the sentence "Mr. Smith did not murder his wife," the humans will still bear the responsibility even though they were powerless to prevent it. This type of liability isn't unprecedented, but it probably hasn't seen widespread use since codpieces were the height of male fashion. (hmmm....)

The bigger problem is that this will be an unbearable temptation to the same "technical solutions to social problems" crowd that loves photo radar and net filters in libraries. Why worry about the attitudes that would make someone type "the N word" if you can require software to automatically edit out the offensive word or phrase? Even better, we even have the precedence that WYSIWYG doesn't mean WYSIWYG - it's now perfectly legitimate for the original author to see what he typed, but for the saved file (and all subsequent viewers) to see a different word.

What would stop the Republic of Freedonia from requiring all word processors replace all references to their breakaway province Catatonia with the phrase "breakaway province of Catatonia"? The Breakaway Province of Catatonia would naturally have its own laws regarding Imperialistic Freedonia.

In the US we have the First Amendment to protect us from laws requiring such

changes. Which just means that these law will sneak in the back door. Some obvious examples: how could any school justify allowing minor students to write obscene screeds? (Never mind legitimate book reports on Mark Twain.) How can any company defend itself against a sexual harassment suit, already an extremely confusing body of case law, if company e-mail allows employees to be referred with "the B and C words?"

This "feature" isn't scary because it will break a few links. It's scary because it opens the door for our voices to become those of a stranger.

Bear Giles [bgiles \(at\) coyotesong \(dot\) com](mailto:bgiles@coyotesong.com)

---

**✶ Re: Office XP modifies what you type (Deegan/Arnold, [RISKS-21.42](#))**

LShaping <nospam@all.please>  
*Fri, 01 Jun 2001 13:15:02 GMT*

Microsoft knows best. That is no different than Windows 95 forcing all capital-letter file names into Microsoft's chosen format. You have no choice, you are not given any way to change the behavior, you must submit to Microsoft's wishes. Must feel good to be a monopoly and be able to force personal computer users to behave as you wish.

---

## **⚡ Re: "Hacker Insurance" charges higher rates for Windows systems!**

Elana Who? <falcospav@excite.com>

*5 Jun 2001 07:54:19 -0700*

Two quotes from the article:

"J.S. Wurzler Underwriting Managers, one of the first companies to offer hacker insurance, has begun charging its clients 5 percent to 15 percent more if they use Microsoft's Windows NT software in their Internet operations. "

"...found that system administrators working on open source systems tend to be better trained and stay with their employers longer than those at firms using Windows software, where turnover can exceed 33 percent per year."

The article can be found at:

<http://www.zdnet.com/intweek/stories/news/0,4164,2766045,00.html>

-Elana

---

## **⚡ Re: UK Government Gateway blocks non-MS browsers (Mistry, R-21.44)**

"David G. Bell" <dbell@zhochaka.demon.co.uk>

*Tue, 05 Jun 2001 07:25:03 +0100 (BST)*

The same system is also being used for the electronic submission of EU

subsidy claim forms to MAFF (the UK's agriculture department), the details of which are available from the [www.maff.gov.uk](http://www.maff.gov.uk) site. While it has been heavily pushed by MAFF, as a consequence of the outbreak of Foot and Mouth Disease in the UK, and a desire to reduce the risk of accidental transfer of the virus by farmers delivering forms to MAFF offices, there is still the problem of getting the certificates.

Also, some of the claim forms require additional documents, such as sketch maps, which cannot be so easily presented as a blank electronic form in a browser. There seems to be a RISK that instead of a large envelope, containing everything and delivered, with tracking, by the Post Office, there is an envelope, and a set of electronic data, which must be connected together somewhere in the MAFF admin system.

There has been some reporting by users, this year and of the trial last year, in the [uk.business.agriculture](http://uk.business.agriculture) newsgroup. The abbreviations "IACS" and "AAPS" will be useful in any searches of news archives.

Incidentally, I had an e-mail discussion, before the trials started, with one of the MAFF personnel involved, about the various open signature and encryption standards defined in RFCs. He had, as I recall, not heard of them.

David G. Bell -- Farmer, SF Fan, Filker, and Punslinger.

## **10th USENIX Security Symposium**

Tiffany Peoples <tiffany@usenix.org>

*Thu, 31 May 2001 16:40:51 -0700*

10th USENIX Security Symposium

August 13-17, 2001

Washington, D.C.

<http://www.usenix.org/events/sec01>

Sponsored by USENIX, the Advanced Computing Systems Association

[www.usenix.org](http://www.usenix.org)

REGISTER BY JULY 20, 2001 AND SAVE UP TO \$200!

PRACTICAL SECURITY FOR THE REAL WORLD

KEYNOTE ADDRESS by Richard M. Smith, CTO, Privacy Foundation

"Web-Enabled Gadgets: Can We Trust Them?"

24 REFEREED PAPERS on the best new research

INVITED TALKS by Matt Blaze, Mark Eckenwiler, Eric Murray,

John Young, Deborah Natsios, etc.

6 TUTORIALS

---

## **16th Annual Software Engineering Symposium 2001**

Carol Biesecker <cb@sei.cmu.edu>

*Sun, 3 Jun 2001 20:13:07 +0000 (UTC)*

SEI 16th Annual Software Engineering Symposium 2001

October 15 - 18, 2001

Grand Hyatt at Washington Center

Washington, D.C.

World Wide Web: <http://www.sei.cmu.edu/symposium/>

Catalysts for Improving Acquisition and Development of  
Software Intensive Systems

Symposium 2001 Conference Coordinator  
412 / 268-3007  
E-mail: [symposium@sei.cmu.edu](mailto:symposium@sei.cmu.edu)

For more information about the Symposium, contact  
Symposium 2001 Conference Coordinator  
Phone: 412 / 268-3007  
FAX: 412 / 268-5556  
E-mail: [symposium@sei.cmu.edu](mailto:symposium@sei.cmu.edu)  
World Wide Web: <http://www.sei.cmu.edu/symposium/>



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 21: Issue 46**

**Tuesday 12 June 2001**

## Contents

- [Another NY Stock Exchange outage](#)  
[PGN](#)
- [California power grid hacked](#)  
[PGN](#)
- [PC parrot drives firemen crazy](#)  
[Merlyn Kline](#)
- [Computer reports unreported wreck](#)  
[Chris Norloff](#)
- [U.K. plans mandatory IP indoctrination for children](#)  
[Cluebot via Declan McCullagh](#)
- [Re: Billboard error message](#)  
[Robert Meineke](#)  
[Rick Prelinger](#)  
[John Dallman](#)
- [Re: Risks of clueless marketing](#)  
[Jamie McCarthy](#)
- [Re: Steve Gibson: Windows XP Vulnerable; Big ISPs just don't care](#)  
[Mike Nuss](#)
- [Re: Steve Gibson's report and Windows XP "Vulnerabilities"](#)  
[David Crooke](#)

- [They're at it again: Internet Explorer Smart Tags in WinXP](#)  
[Stef Maruch](#)
  - [Re: Office XP modifies what you type](#)  
[Andy Newman](#)  
[Jay Jennings](#)
  - [Microsoft, 'Mitigating Factors' and Public Relations](#)  
[Jackson Ratcliffe](#)
  - [Broken shopping carts](#)  
[Steve Loughran](#)
  - [How to avoid Internet interruption at AAS meeting](#)  
[Clive Page](#)
  - [There's no such thing as software `piracy'](#)  
[Fred Gilham](#)
  - [Re: Another fear of Risks](#)  
[James K. Huggins](#)
  - [Re: McDonald's testing cashless payments](#)  
[Jeffrey Jonas](#)  
[John R Levine](#)
  - [Credit where it isn't due](#)  
[William Paul Fiefer](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

## ⚡ Another NY Stock Exchange outage

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

*Fri, 8 Jun 2001 19:21:22 PDT*

A software upgrade glitch resulted in the New York Stock Exchange being unable to trade roughly half of its stocks in the morning of 8 Jun 2001. Consequently, the exchange was shut down entirely (on grounds of fairness) until 11:35 a.m. EDT.

The RISKS archives note a 41-minute shutdown on 24 Feb 1971

(when both primary and backup systems failed), a 24-minute outage on 22 Oct 1991 (due to a power dip), a one-hour outage on 18 Dec 1995 (also due to a botched software update), and a one-hour crash on 26 Oct 1998. Uninterrupted service is clearly not easy to achieve. The Nasdaq exchange computer system also shut down last week for 20 minutes (while the staff was working to increase capacity), a case that has not previously been reported here.

---

## **California power grid hacked**

"Peter G. Neumann" <neumann@csl.sri.com>  
*Tue, 12 Jun 2001 08:13:22 -0700*

Reuters reported on 11 June 2001 that the California Independent System Operator's flow-control computer systems had been hacked for at least 17 days before it was detected on 11 May 2001 -- in the midst of the ongoing power crisis. Although they attacks did not noticeably disrupt operations, they apparently came quite close -- and exposed some vulnerabilities that demonstrably need to be fixed. The main attack was seemingly from someone in China's Guangdong province, via China Telecom, and exploited Internet servers in Tulsa OK and Santa Clara CA.

---

## **PC parrot drives firemen crazy**

"Merlyn Kline" <merlyn@zynet.net>

*Thu, 7 Jun 2001 13:08:17 +0100*

In an article in *\*The Register\**, Kieren McCarthy  
<<http://www.theregister.co.uk/content/28/19525.html>>  
reported that West Midlands firemen, having rescued a cat from a  
tree, were  
called to an office in Willenhall to rescue what was thought to  
be an  
escaped parrot. After an hour's search, they discovered that a  
PC  
screensaver was intermittently parroting a parrot's squawks.  
Kieren  
speculated on whether the firemen thought it was a joke or "more  
reasonably,  
smashed the PC to pieces with their axes." [Merlyn called this  
a "terrible  
parrot error", although I doubt that the firemen thought it was  
a parody.  
Instead, it was truly a case of a polly-morphic PC! PGN-ed]

---

## **Computer reports unreported wreck**

"Chris Norloff" <cnorloff@norloff.com>

*Thu, 7 Jun 2001 08:44:52 -0400*

You just can't outrun a satellite. A Merced, California, man  
took his fully  
equipped 2001 SUV out onto some nearby country roads, navigating  
swiftly and  
confidently with the optional OnStar Global Positioning System.  
When he got  
into an accident, he decided to run for it. But the guidance  
system had  
already notified OnStar headquarters of the accident, specifying

where it had happened and giving a complete description of his vehicle to the California Highway Patrol. The officers followed a trail of coolant about a mile into an orchard, where they found and arrested the driver.

[Source:

\*Road & Track\* magazine, July 2001; PGN-ed]

THE RISKS?

What constitutes an "accident"? (Air bags seem to go off quite easily, taking out the windshield and dashboard [\$\$\$] in a fender-bender).

Will GPS-reported accidents become like household burglar alarms - sending out mostly false alarms?

Who will hack into the OnStar system to falsely report accidents?

Who will use the OnStar system to efficiently dispatch lawyers to accident sites?

How soon until OnStar sells accident records so used-car purchasers can learn the vehicle's history?

Chris Norloff

---

## **✶ U.K. plans mandatory IP indoctrination for children (from Cluebot)**

Declan McCullagh <declan@well.com>

Wed, 6 Jun 2001 12:17:49 -0400

<http://www.cluebot.com/article.pl?sid=01/06/05/2338246>

U.K. Plans Mandatory IP Indoctrination for Children  
posted by vergil on Wednesday June 06, @12:10PM  
from the get-em-while-they're-young dept.

Forget digital watermarks and cease-and-desist letters. The future of intellectual property enforcement lies not in technological access controls or litigation, but mandatory education. Anthony Murphy, the UK Patent Office's Director of Copyright since 1999, has hit upon a novel solution to stamp out public disregard for copyright law by nipping future file-swappers in the bud.

In a move that's an eerie cross between Brave New World and the Lehman Working Group's "Just Say Yes" (to licensing) proposal, the UK's Patent Office and Department of Education have teamed up to teach youngsters the virtues of copyright. Starting in fall 2002, reverence to intellectual property -- and, presumably, disdain for Napster and its successors -- will become part the "Citizenship" aspect of England's National Curriculum for secondary school students.

According to a April 26, 2001 UK Patent Office press release:

"In Autumn 2002, a new subject, Citizenship, is being introduced into the National Curriculum in UK secondary schools. Its aim is to teach children how to be good, moral, citizens and Anthony Murphy believes the subject would be an ideal vehicle for teaching children about intellectual property.

'By bringing awareness of the importance of copyright into our schools, tomorrow's consumers can take their place in a community which understands, values and respects intellectual property.' "

POLITECH -- Declan McCullagh's politics and technology mailing list

You may redistribute this message freely if you include this notice.

To subscribe, visit <http://www.politechbot.com/info/subscribe.html>

This message is archived at <http://www.politechbot.com/>

---

## **⚡ Re: Billboard error message (PGN, [RISKS-21.45](#))**

"Robert Meineke" <robert\_meineke@hotmail.com>

*Thu, 07 Jun 2001 09:02:06 -0700*

Just for fun, check out

<http://www.daimyo.org/bsod/>

[This Web site shows some classic blue screens of death in very conspicuous places. PGN]

---

## **⚡ Re: Billboard error messages (PGN, [RISKS-21.45](#))**

Rick Prelinger <footage@panix.com>

*Thu, 7 Jun 2001 11:15:50 -0700*

The best CalTrans error message I have seen was sometime last fall on the San Francisco approach to the Golden Gate Bridge, where an

industrious purple LED sign repeatedly flashed "NO DATA."

Rick Prelinger, Prelinger Archives, P.O. Box 590622, San Francisco, Calif.

94159-0622 +1 415 750-0445 <http://www.prelinger.com>  
footage@panix.com

---

**✶ Re: Billboard error message (PGN, [RISKS-21.45](#))**

John Dallman <jgd@cix.co.uk>

*Fri, 8 Jun 2001 00:16 +0100 (BST)*

My personal favourite was the time I found a hole-in-the-wall cash dispenser that had fallen over and was displaying a "C:>" prompt. A little playing with the keyboard revealed that MS-DOS was running - or something else that said "Bad command or file name" - and the keypad gave me numbers, ESC, BACKSPACE and ENTER. With no ALT key or letters, I couldn't do more, so the design had some limited degree of fail-safety.

John Dallman <jgd@cix.co.uk>

---

**✶ Re: Risks of clueless marketing (Searle, [RISKS-21.44](#))**

Jamie McCarthy <jamie@mccarthy.vg>

*Mon, 4 Jun 2001 21:57:48 -0400*

> Has anybody else realized that "XP" is a person wincing [...]?

This is the company that named an earlier operating system "WinCE".

Maybe their \*market\* is people with pained facial expressions.

---

## **✶ Re: Steve Gibson: Windows XP Vulnerable; Big ISPs just don't care**

Mike Nuss <nmx@fromtheshadows.net>

*Thu, 07 Jun 2001 16:46:45 -0400*

I felt I had to respond to this article, because it's simply ridiculous.

Raw sockets support, the supposed "vulnerability," is not a security risk. This capability is already present in every major Unix operating system, and can be acquired in every version of Windows with the addition of a library.

From atstake.com:

The "powerful Internet-connection capabilities" which are hyped in this

article is merely the ability to write raw IP packets. This is where an

application program controls every field in the IP packet. This functionality is required if you were writing your own network bridge

program for Windows or other low level network applications. An IDS for NT

that resets connections would need this functionality. AntiSniff, which

detects sniffers on a network, requires this functionality.

This capability, which this article states is so dangerous to the

Internet, is already available practically everywhere. It is available in

every commercial and open source unix distribution and is already

available for all Windows platforms (not just Windows XP) through the use

of free add on libraries such as winpcap and libnetNT.

The hype and hyperbole is astounding. From reading this article you'd

think a deluge of DDoS attacks was building up just waiting to be released

once Microsoft releases the all powerful new API. Nothing could be further

from the truth. When XP arrives it will receive a collective yawn from

DDoS attackers who would much rather have their win32 DDoS clients run on

every version of Windows using the already available add on libraries.

Once an attacker has administrative control of a machine they can run any

code they want, whether it is native or in an uploaded executable. There

is absolutely nothing stopping an attacker from spoofing IP addresses from

a Windows machine today or tomorrow.

The real RISK here is \*The New York Times'\* propagation of false information

for the sole purpose of provoking Fear, Uncertainty, and Doubt.

Mike Nuss

---

## ⚡ Re: Steve Gibson's report and Windows XP "Vulnerabilities"

David Crooke <dave@convio.com>

Thu, 07 Jun 2001 00:48:25 -0500

I have to take issue with Steve's assessment of how important

this new capability in Windows 2000 / XP is - given the technical mastery required to subvert a machine in the first place, it's not a major endeavour to implement one's own source IP spoofing in any number of ways - a second virtual interface, bundling a custom IP stack with the trojan, or just changing the IP address of the machine. The fact that most current attacks don't use IP spoofing is not because Microsoft has failed to provide a convenient API - attackers simply haven't felt the need. Other operating systems have "supported" IP spoofing for years without it being regarded as risk contributing to hacking efforts.

The real takeaway from Steve's write-up is that the endpoints of the Internet can no longer be trusted; it is time for network administrators at ISPs, universities and commercial premises to take up the cudgel and police the traffic emanating from their networks; source IP filtering is trivial to implement at this level. It is also time for backbone providers to introduce sensible firebreaks and reduce their trust in traffic passing through their systems.

---

## **⚡ They're at it again: Internet Explorer Smart Tags in WinXP**

Stef Maruch <stef@cat-and-dragon.com>

*Thu, 7 Jun 2001 12:55:52 -0700*

A while back, when www.deja.com still archived Usenet news, they tried to generate revenue by inserting URLs into Usenet posts archived on their site. Needless to say, this upset a lot of Usenet posters, who considered it a copyright violation.

Now Microsoft is up to much the same thing with a new feature of WinXP called "Internet Explorer Smart Tags":

<http://public.wsj.com/sn/y/SB991862595554629527.html>

In effect, Microsoft will be able, through the browser, to re-edit anybody's site, without the owner's knowledge or permission, in a way that tempts users to leave and go to a Microsoft-chosen site -- whether or not that site offers better information.

Seems to me they should be called "Internet Explorer Sneak Tags."

Stef \*\* rational/scientific/philosophical/mystical/magical/  
kitty  
\*\* stef@cat-and-dragon.com <\*> <http://www.cat-and-dragon.com/~stef>

\*\*

I mean, 'e' was *\*already\** the most common letter in the English language. -- AM, complaining about the online commerce explosion

---

## **⚡ Re: Office XP modifies what you type (Deegan/Arnold, [RISKS-21.42](#))**

Andy Newman <andy@silverbrook.com.au>  
Thu, 7 Jun 2001 18:41:07 +1000

When I saw the headline I thought "Oh, oh, MS at it again" but after reading further on must agree with what they're doing. A quick glance at an appropriate RFC - 2396, Uniform Resource Identifiers: Generic Syntax - shows that forward slash is reserved within URI paths and may not appear twice in succession. I quote,

The path may consist of a sequence of path segments separated by a single slash "/" character. Within a path segment, the characters "/", ";", "=", and "?" are reserved.

Also having written a few simple web servers and many robots I find the claim that there are many uses of '//' rather dubious. The people are probably thinking that some kind server's path normalisation is normal or the laziness of many HTTP server authors in transforming "entity" paths into the names of files storing those entities makes their invalid URLs allowable.

I think the real risk of URLs (and I's and N's) is that they appear too similar to the names used in many file systems. This leads to things like thinking '//' in the middle of a path is valid (hey Unix copes!) or that ".jpg" on the end of a URL actually means something and you can ignore the entity type sent back with the data (common browser problem).

Andy Newman, Silverbrook Research, <andy@silverbrook.com.au>

## **✶ Re: Office XP modifies what you type (Deegan/Arnold, [RISKS-21.42](#))**

"Jennings, Jay" <jay.jennings@capitalone.com>

*Thu, 7 Jun 2001 15:24:18 -0400*

Two interesting points. First, in previous versions of Microsoft Word, the feature that changed capital letters could be turned off - it was called the "Auto Correct" feature and could be tweaked through the tools menu. The second point is more ironic. I received the link below in an e-mail yesterday:

[http://shop.microsoft.com//Products/Products\\_Feed/Online/SQLServer2000%5B101/ProductQuestions.asp](http://shop.microsoft.com//Products/Products_Feed/Online/SQLServer2000%5B101/ProductQuestions.asp)

I was quickly able to deduce that Office XP was not used to compose the e-mail.

Jay Jennings

---

## **✶ Microsoft, 'Mitigating Factors' and Public Relations**

"Ratcliffe, Jackson" <jratcliffe@vlg.com>

*Thu, 7 Jun 2001 07:39:45 -0700*

Microsoft recently announced yet another security flaw, this one related to Exchange 2000's Outlook Web Access (OWA). Apparently java/vbscript attachments are automatically run

<http://www.microsoft.com/technet/security/bulletin/MS01-030.asp>  
with no security. This is a REAL glaring flaw.

So to make sure that it doesn't sound quite so bad, in Microsoft's e-mail announcement they tried to list the mitigating factors. Have a laugh.

Mitigating Factors:

- The vulnerability could only be exploited if the user were using OWA in conjunction with IE. (isn't that the whole point of the product ?)

- The vulnerability is only exploitable by attachments that are received via OWA. In general, an attacker would have no way to determine whether a user would open an attachment using OWA rather than an Outlook client. (Isn't the whole point of .net to get rid of client-based Outlook?)

[CC:ed on this item by Jackson, Gregory D. Marx concludes that

"based on the first mitigating factor, I guess MS is suggesting that we switch to Netscape!?!?" PGN]

---

## ✶ Broken shopping carts

"Steve Loughran" <slo4@iseran.com>  
*Wed, 6 Jun 2001 22:56:34 -0700*

I was just trying to buy something from an on-line catalog (autosport.com), but was having problems as the shopping cart doubled the number

of items I  
entered; the minimum purchase was two.

On a whim, I entered a negative number -and the shopping cart  
updated to  
show that I was ordering -2 items, and had to pay -\$188.

I didn't go ahead with the transaction, but it would be an  
interesting  
experiment to see whether it would actually be possible to get  
free cash  
from shopping at this web site.

It would also be interesting to see if the credit card companies  
fraud  
protection works in reverse -detecting and flagging too many  
refunds coming  
from a single vendor.

---

## **⚡ How to avoid Internet interruption at AAS meeting**

Clive Page <cgp@leicester.ac.uk>  
*Mon, 4 Jun 2001 16:07:56 +0100*

Astronomers planning to attend the American Astronomical Society  
meeting  
on now were advised as follows in an e-mail circular:

If you plan on attending the AAS Meeting in Pasadena, CA 3-7  
June 2001,  
you will most likely want to use the Meeting's Cyber Cafe for  
E-mail and  
Web Browsing. In order to ensure continuous access to your  
home site,  
please notify your local system and security administrators of  
the  
following:

The Internet traffic flowing from the meeting attendees, will

be coming

from the IP addresses ranging from [CENSORED... actual  
addresses removed  
for obvious reasons].

In the past government sites have become aware of heavy  
traffic from our  
meetings and without notice shut off ALL access to attendees.  
This was  
done as a security measure, unaware that the traffic was  
originating at an  
AAS Annual Meeting. It caused several days of service  
interruption for  
meeting registrants. Informing your system administrators of  
the IP  
addresses could save you a lot of distress later!

The risk: trying to avoid denial-of-service attacks might cause  
almost as  
much disruption to your staff as an actual attack, and just when  
they are  
least likely to be able to do much about it.

Clive Page, Dept of Physics & Astronomy, University of  
Leicester. U.K.

---

## **⚡ There's no such thing as software `piracy'**

Fred Gilham <gilham@csl.sri.com>  
*Tue, 05 Jun 2001 10:12:33 -0700*

I know it's not a new idea, but I think it needs to be  
reiterated that  
piracy (which apparently is still practiced in some parts of the  
world) is a  
crime of violence, often resulting in the death of its victims,  
whereas  
making unauthorized copies of software that is copyright or

licensed, while  
illegal in most places, is not a crime of violence.

It may be tilting at windmills, like trying to get people to use  
the term  
'crackers' instead of 'hackers'. Perhaps the people who write  
stories about  
this stuff would be more careful with their terminology if  
people started  
referring to 'taggers' (i.e., graffiti vandals) as  
'journalists'? After  
all, they both work with words....

---

## ✶ Re: Another fear of Risks

James K. Huggins <huggins@quip.eecs.umich.edu>  
*31 May 2001 10:18:07 -0400*

Sorry ... here I go on a rant ...

"Bob Frankston" <rmf2g0ther@bobf.Frankston.com> writes:

> I'm using IE 6.0 and it works pretty much like 5.0. With one  
> notable  
> exception -- UPS explicitly checks for it and doesn't let me  
> use their  
> service with an unapproved browser. I presume that feel it is  
> better for  
> them to lose customers than risk .. risk what?

Risk spending countless hours of time on the phone (and  
therefore \$\$) with  
irate customers blaming UPS when the customers' new-fangled  
"compatible"  
browser doesn't work with the UPS site. Risk having people  
blame UPS  
instead of Microsoft when IE 6.0 turns out to not be 100%  
compatible with IE  
5.x in a couple of features which the UPS cite depends upon to

function  
correctly ... especially if those incompatibilities didn't  
surface in any of  
the pre-release versions.

> UPS is loses two ways. They force me to use other services and  
they  
> lose the value of users doing testing for them.

In my humble opinion, most users aren't interested in doing  
testing  
for companies. That's what we pay the companies to do for  
themselves.

Furthermore, relying on user reports for testing is full of its  
own  
problems. Users (and I count myself in that category) will often  
blame others for problems they cause themselves, or problems  
caused by  
third parties (e.g. ISPs) which aren't the fault of either  
endpoint.

> They can warn me that they haven't tested with my browser but  
> disallowing it is not only short-sighted, it represents a basic  
> misunderstanding of the PC and the large effort put in to  
assure  
> compatibility with previous versions of programs.

Who says UPS won't eventually support IE 6.0? Given that it's  
just  
been released, UPS may just be trying to give itself some time to  
test IE 6.0 for itself and fix any compatibility problems on its  
end.

> Old MIS (before they were called IT) departments did have a  
great  
> fear of upgrades since each mainframe system was extensively  
> patched. But that reasonable fear is now a phobia.

Nope. Look, I've had much the same problem with the Netscape 4-  
>6  
transition. When I upgraded to the "improved" Netscape 6 on my  
home

machine, lots of sites that I used to visit simply refused to work anymore. When I contacted the sites to complain, most state that the problem is Netscape's and that I should either downgrade back to 4.72 or switch to IE.

There ain't nothing that's 100% backward compatible, especially in a x.0 release.

Just my \$.02.

--Jim Huggins, Kettering University, Flint, MI  
(jhuggins@kettering.edu)

---

## ✦ **Re: McDonald's testing cashless payments ([RISKS-21.43](#))**

Jeffrey Jonas <jeffj@panix.com>  
*Tue, 29 May 2001 22:11:30 -0400 (EDT)*

> McDonald's Corporation has begun testing the use of a cashless payment  
> system that uses the kind of radio transponder technology that was first  
> developed by state highways to allow motorists to drive through toll plazas  
> without having to stop to make a payment.

A friend said that McD's once had a credit card but dropped it. Sure, it made checkouts faster and less handling of cash, but it had an unexpected side effect. Folks saw the monthly bill and realized how all those meals were adding up to real money and cut back their spending since it was so easily auditable.

Another interesting interaction:

> Newsgroups: alt.consumers.experiences,misc.consumers  
> Subject: Re: McDonald's 30-Second DT Guarantee

McD's apparently has some promotion where they guarantee you get the food

30 seconds after paying. The immediate analysis is that they'll take

as long as before, just not collect the money 'till it's ready. Now with the speed-pass, will the guarantee still hold?

---

## ⚡ Re: McDonald's testing cashless payments ([RISKS-21.43](#))

"John R Levine" <johnl@iecc.com>

*30 May 2001 02:26:29 -0400*

I had a Mobil speedpass for a while. It's about the diameter of a pencil

and an inch long, with a hole through the end so it can go on your keychain.

You wave it at the pump, a light on the pump goes on to tell you it knows

who you are and you pump your gas. Mobil links theirs to a credit card.

It worked fine until one day my bank called me up to say that I had been

buying an awful lot of gas in towns east of here, had I lost my card?

No, but it turned out that I'd lost my speedpass. It fell off my keychain

the last time I used it, but it was so small that I didn't notice it was

gone, what with all the frequent shopper barcode tags et al with my keys.

I finally got it straightened out and Mobil ate the bogus charges, a

relief since the card company said their usual anti-fraud rules don't

apply when you don't use your physical card for a transaction.

I decided I'll spend the extra two seconds per visit and swipe my card.

I do have an E-ZPass toll transponder in my truck, but that's different for two reasons: it's large enough to miss and is firmly glued to the inside of the windshield, and they give me the incentive of significant toll discounts (in NYC at least) if I use it.

John Levine, johnl@iecc.com, Primary Perpetrator of "The Internet for Dummies", Information Superhighwayman wanna-be, <http://iecc.com/johnl>, Sewer Commissioner

---

## ✶ Credit where it isn't due

William Paul Fiefer <yamada@prairienet.org>

*Wed, 06 Jun 2001 19:55:27 -0500*

So you request a credit card and it comes by mail with a peel-off sticker across the signature plate. The sticker tells you to call a toll-free number to activate the card. This is, apparently, a theft-prevention thing.

Don't bother.

The cards activate automatically. At least "Blue" from American Express and the "Platinum" series (\$100,000 credit limit -- \$250,000 for the "Quantum" series) from MBNA do.

I ordered these cards but did not activate them. I found myself receiving mail regarding these accounts. I received privacy notices, which I opted out of. Then I asked MBNA why I had a card I did not activate.

If you do not activate our cards, the customer rep said, they activate themselves after a set time limit. The American Express rep told me no such activation occurred but could not explain why my card was active. She even tried to discourage me from cancelling the thing!

The RISK? You'll have credit due where none is applied for.

William Paul Fiefer 630.892.5180 [www.prairienet.org/~yamada](http://www.prairienet.org/~yamada)



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 21: Issue 47**

**Wednesday 13 June 2001**

## Contents

- [Computer train trauma](#)  
[Lord Wodehouse](#)
- [Elevator emergency override drowns woman](#)  
[Daniel Norton](#)
- [ATM network center flooded](#)  
[Daniel Norton](#)
- [Supreme Court ruling on thermal-imaging scanners](#)  
[PGN](#)
- [And you thought Keith Lynch was kidding!](#)  
[PGN](#)
- [DoD declares unclassified hard drives no longer need be destroyed](#)  
[PGN](#)
- [Risks of URL-forwarding services](#)  
[Justin Mason](#)
- [New technology for sneaky advertising](#)  
[Greg Searle](#)
- [ScanMail's "sophisticated" filtering blocks PRIVACY Forum Digest](#)  
[Lauren Weinstein](#)
- [Risks of heuristics and marketers](#)  
[Dan Birchall](#)

- [Re: Dutch government to act against virtual child pornography](#)  
[George Dinwiddie](#)
  - [Security notice for recent EarthBrowser purchasers](#)  
[Matt Giger via Ben Laurie](#)
  - [Excel date munging: what a difference --four years and-- a day makes](#)  
[Tom Walker](#)
  - [Dead men produce no documentation](#)  
[Kirt Dankmyer](#)
  - [REVIEW: "Inside Internet Security", Jeff Crume](#)  
[Rob Slade](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

## ✶ Computer train trauma

Lord Wodehouse <w0400@ggr.co.uk>

Tue, 12 Jun 2001 13:10:42 +0100

>From \*Computer Weekly\* 7 Jun 2001, on the back page.

... a tale of cutting edge IT going off the rails.

It reads, "I had an interesting journey home from London last night. I was onboard a new 100% computer-controlled train. In the middle of the Chester countryside, the train ground to a halt. The automated station-announcement system then ran through its program of station announcements in quick succession until it said the final destination."

"It then attempted to open the doors (in the middle of nowhere). The guard ran to the driver's cab. The driver and the guard then ran through the carriages muttering that the computer had gone berserk and was telling them that the rear of the train was on fire. After checking, the

driver, in a state of mild panic ran back to the cab, turned off all the engines, cut off all the power (leaving us in pitch darkness), and yes, you've guessed it, waited the customary - 10 seconds and rebooted the train.

I wonder if anyone can confirm this wonderful story. The risks are self-evident.

SCS Global Services Internet/Intranet Operations,  
GlaxoSmithKline,  
Medicines Research Centre, Gunnels Wood Road, Stevenage SG1 2NY  
UK

---

## **⚡ Elevator emergency override drowns woman**

Daniel Norton <Daniel@DanielNorton.net>

*Sun, 10 Jun 2001 20:50:28 -0400*

cf. <http://www.chron.com/cs/CDA/story.hts/metropolitan/936841>

Though not mentioned in this article from the \*Houston Chronicle\*, NPR reported (via KUHF?) that the elevator detected an emergency situation and automatically attempted to move to the ground floor. While that's often a good idea in case of a fire, in a flood it's the \*worst\* way to respond and, in this case, tragically lethal.

[I was in an elevator at BBN in Rosslyn VA once when the control computer crashed. The elevator very slowly worked its way to the TOP floor, which might seem to make sense -- \*except\* in a fire. Thus, we need

an

intelligent system that figures out which way to go, and therein lie even

more risks -- especially in a fire that results from a short caused by a flood. PGN]

---

## ✂ ATM network center flooded

Daniel Norton <Daniel@DanielNorton.net>

*Sun, 10 Jun 2001 20:59:46 -0400*

The Pulse EFT network's main and backup power systems in Houston were flooded by Tropical Storm Allison, disabling their 22-state ATM network.

"PULSE Enacts Disaster Recovery Program

Early Saturday morning, the PULSE electronic funds transfer system

experienced a major disruption of both our primary power source and our

emergency back-up supply system, as a result of unprecedented flooding in

Houston. A disaster recovery program has been instituted and efforts are

underway to resume operations at a remote processing center located in

Dallas. Until technical connections in the system can be restored,

disruption of ATM and point-of-sale services at some locations will be

experienced. PULSE has a proud record of 99.99% availability and we

regret any inconvenience to our financial institutions, merchants,

processors and cardholders that this extraordinary event may have caused.

[...] <http://www.pulse-eft.com/>

---

## ✶ Supreme Court ruling on thermal-imaging scanners

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

*Tue, 12 Jun 2001 12:12:13 -0700 (PDT)*

In the *Kyllo* case, the Supreme Court ruled 5 to 4 that using an Agema 210 thermal-imaging device to scan for unusual heat sources in someone's house (i.e., searching for marijuana growing activities) is unlawful search if carried out without a warrant, violating the Fourth Amendment.

<http://www.supremecourtus.gov/opinions/00slipopinion.html>

<http://supct.law.cornell.edu/supct/html/99-8508.ZS.html>

<http://www.wired.com/news/politics/0,1283,44444,00.html>

---

## ✶ And you thought Keith Lynch was kidding! (Re: [RISKS-21.42](#))

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

*Mon, 12 Jun 2001 12:17:11 -0700 (PDT)*

<http://www.utm.edu/research/primes/curios/48565...29443.html>

One of the strangest consequences of the DMCA is that it would seem to outlaw possession of certain integers. The above URL gives the decimal form of a prime number whose HEX form just happens to be the gzip-ed C source code for DeCSS (which breaks the DVD Movie encryption -- see

[RISKS-21.37](#)).

This observation is due to Phil Carmody.

[Thanks to Mark Brader for the Subject: line!]

---

## ⚡ DoD declares unclassified hard drives no longer need be destroyed

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

*Sat, 9 Jun 2001 23:17:52 -0700 (PDT)*

<http://www.cnn.com/2001/TECH/ptech/06/08/pentagon.computers.ap/index.html>

The aggregation, inference, and sensitive-unclassified stuff is ubiquitous and often damning. This could be a harbinger of future RISKS stories.

---

## ⚡ Risks of URL-forwarding services

Justin Mason <jm-risks@jmason.org>

*Thu, 07 Jun 2001 12:44:09 +0100*

I'm the maintainer of a free-software application called sitescooper, which reformats Web sites for viewing on PDAs. When I started writing sitescooper a few years ago, I hosted it on my ISP at <http://www.clubi.ie/~jmason/software/sitescooper/>.

Since this URL was quite cumbersome (especially when read on a PDA screen!)

I also set up a forwarding URL with a domain called "tsx.org", which offered free URL forwarding. At that stage, tsx.org was a reasonably reputable URL-forwarding service.

Since then, sitescooper has grown in popularity, and has moved to the easier-to-remember sitescooper.org domain. I left the tsx.org forwarding in place, updated to its new address, to catch old links and avoid link-rot, and forgot about it.

This morning I received a mail from a potential user, who'd decided to download sitescooper and take a look. The mail stated:

I'm writing about your Web site. [...]

If you are aware of the way your site behaves then you should just close up shop and leave the Web because no contribution to software development is worth the hassle your site causes.

If not, then I apologize for the above and I'll describe it for you.

If your site: sitescooper.tsx.org is opened using a script-enabled browser (e.g., IE or NS), from a windows platform, it proceeds to plaster the screen with windows full of trashy ads that CANNOT be deleted. The windows have no controls and right-clicking the taskbar icons is disabled. THE ONLY WAY to delete this trash is to bring up the Task Manager via ctrl-alt-del, and kill the processes. NO WEBSITE SHOULD BE THIS INVASIVE.

This is blatant abuse of the trust a user puts in you when they click a link to your site. Hopefully, you're not involved in it and it's being done by tsx - In which case I STRONGLY advise you to dump them as fast as possible and find a new Web host.

I surfed over to sitescooper.tsx.org and took a look. Sure enough, it popped up 5 windows - 1 with no frame masquerading as a Windows alert, asking if I want to visit the BEST ADULT SITES AROUND, 2 full-screen unclosable windows, 1 normal(ish) ad window with a normal window frame, and (finally) the page I \*wanted\* to go to.

Gah. Needless to say, sitescooper.tsx.org is now no more. I'd prefer if people hit a 404, and were forced to search Google, than run into this.

The risk? There ain't no such thing as a free lunch, I guess. I'd assumed that the forwarding system would offer a consistent quality of service over several years; instead, in my opinion, they took advantage of their situation to increase their ad revenues at the expense of their users.

---

## **✶ New technology for sneaky advertising**

"Greg Searle" <gsearle@s1.com>  
*Thu, 7 Jun 2001 14:42:57 -0400*

First came SPAM, with its authors finding more and more sophisticated

methods of hiding themselves from their victims so they could send out massive amounts of advertising without fear of retribution. Then came pop-up window ads. These are bad enough, but now a company, [www.fastclick.com](http://www.fastclick.com), has come up with a way to sneak these pop-up windows onto your screen without you knowing where they came from. Worse, established corporations such as The NY Times ([www.nytimes.com](http://www.nytimes.com)), AltaVista ([www.altavista.com](http://www.altavista.com)), and Epinions ([www.epinions.com](http://www.epinions.com)) are using the technology.

The trick involves a timer, a cookie, and a pop-up window that quickly hides itself \*behind\* your browser windows. This usually happens too fast for your computer to render the window on your display, so you see nothing. You don't know when the ad will appear, and you won't see it until you close all of your browser windows. By then, you have opened a few more windows and browsed to other Web sites. This keeps you from knowing which Web site spawned the window in the first place. I only know about the above three corporations because I was lucky enough to catch the window popping up when I first opened my browser to these sites, or because it was the only site I went to. I caught a glimpse of "fastclick.net" in the status bar, and it all fell into place.

The only solution is to turn JavaScript off completely. If you don't want to do this, then add the offending sites to your "Restricted Sites" list. I have sent a complaint to these corporations as well, letting them know that I don't appreciate this "sneaky" advertising, and have disabled

these ads.

---

## ✶ ScanMail's "sophisticated" filtering blocks PRIVACY Forum Digest

Lauren Weinstein <lauren@vortex.com>

*Sun, 10 Jun 2001 09:46:49 -0700 (PDT)*

Greetings. The manufacturers of e-mail filtering and blocking systems continue to claim that their products have vastly improved over time --that the incidents of false negatives and false positives are greatly reduced from earlier versions. Much empirical evidence has continued in general to contradict these assertions, and here's yet another example of what happens in the real world as these systems are actually configured by users.

My most recent PRIVACY Forum Digest was blocked by the popular "ScanMail" product as configured within at least one site. I only learned about this since the particular configuration was in a "quarantine for review" mode that sent out a warning. Other sites may be configured to simply delete flagged messages without such a reply to the sender.

What was it about the PRIVACY Forum Digest that aroused ScanMail's ire? In the nine years since I originated the Digest, each issue has included a "quote of the day"--which usually is an interesting or amusing quote from a feature film. In the case of the most recent Digest

(<http://www.vortex.com/privacy/priv.10.04>) I chose a quote from Peter Sellers' 1968 classic "I Love You, Alice B. Toklas!"

Ah hah! The phrase "I Love You" appeared in the text of the message. It must be a virus! Or perhaps a spam? Indeed, the Digest was blocked via ScanMail's "ILOVEYOU" policy! This was done even though the message was not encoded in any way and was not an attachment. It was just simple, plain, ordinary, ASCII text, with the "offending" phrase well down within the message (not in the header).

Presumably, ScanMail at various sites will be blocking \*this\* issue of RISKS because (horrors!) the forbidden phrase "I Love You" appears in this message as well!

With such a level of "stone club" analysis at work, one can only imagine what other innocent e-mail is being injected, inspected, detected, infected, neglected, and selected by the "sophisticated" algorithms of filtering programs to be flagged, reviewed, dropped, banned, burned, or trashed.

Lauren Weinstein <lauren@pfir.org> lauren@vortex.com  
lauren@privacyforum.org

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

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

---

## **⚡ Risks of heuristics and marketers**

Dan Birchall <djb@scream.org>

Wed, 6 Jun 2001 18:04:36 -1000

For some years, I have been concurrently involved in countering spam and in designing, implementing and administering e-mail lists for marketing purposes. In both of these endeavors, as in much of life, heuristic (trial-and-error) methods are commonplace.

Heuristic approaches to the development of spam filters tend to be somewhat effective. If one receives 100 pieces of spam over a reasonable period of time containing a given word or phrase, and no legitimate mail containing it, it is statistically probable that filtering mail based on that word or phrase will block at least some spam, and little or no legitimate mail, going forward.

Of course, such simple heuristics are not without their risks. We recently sent an issue of our periodic customer newsletter which contained the phrase "sizzling summer." The marketers love their alliteration -- in fact, the exact same phrase appeared a few days earlier in a mailing by another company in our market segment!

Unfortunately, a small number of sites using simple heuristic filtering like that I described above took offense at our use of the word "sizzling," which apparently now indicates pornographic material.

A better method might combine heuristics with the scoring capability in some mail server software (I'm personally familiar with Exim),

incrementing or  
decrementing a counter based on the occurrence of given words or  
phrases,  
with actions depending on the final value of the counter. Thus,  
if  
"sizzling" is a +1 word, "video" a +2 word, and "sex" a +3 word,  
a threshold  
of 3, 4 or 5 might be used for blocking.

Dan Birchall - Palolo Valley - Honolulu HI - <http://dan.scream.org/>

Peruse my opinions, at <http://dbirchall.epinions.com/user-dbirchall>

[Still too many false positives and false negatives. PGN]

---

## **✶ Re: Dutch government and virtual child pornography (de Geus, R-21.45)**

"Dinwiddie, George" <George.Dinwiddie@arbitron.com>

*Thu, 7 Jun 2001 10:20:31 -0400*

How do you ascertain the age of a virtual individual in an electronically synthesized image? In the real world, you can ask for some identification.

My sister was frequently carded in bars (when the legal drinking age was 18)

until she was 26, because she looked young. My son told me a story of not

being carded at 16 when the guy in front of him was carded at 20 (when the

legal drinking age was 21). Obviously you cannot reliably determine age by

appearances. Perhaps you could look at the creation date of the file? ;-)

[That's not very reliable either. PGN]

---

## **✦ Security notice for recent EarthBrowser purchasers (via Ben Laurie)**

Matt Giger <mgiger@lunarsoft.com>

Wed, 6 Jun 2001 21:49:05 -0700

My name is Matt Giger and I write the EarthBrowser software that you have recently purchased us. I am writing to inform you of about a recent scam being run on our customers. This first report was about 5 PM on 6/6/01 from a customer who purchased EarthBrowser just yesterday.

Apparently some files with customer information on our server have been accessed. Let me assure you that your credit card information is safe since we never store that information on our server. Also we purge all customer information on a daily basis so the amount of information they obtained was minimal, just your name, address, e-mail address and EarthBrowser serial number.

The reported scam e-mail looks something like this:

Please confirm [its] registration. Correct Purchase Information You

account: <http://www.earthbrowser.by.ru/3004001065-010605214102678/index.htm>

This poorly written e-mail sends you to a Web site in Russia which is an exact copy of our purchase page and presumably sends the information you

enter to the thief. If you enter your credit card number on this page, they will then have it so please do not enter any information. Hopefully the poorly worded e-mail and the suspicious Web address will alert most to the fact that this is bogus.

If you have received an e-mail like this one, please let me know as soon as possible so I can trace exactly how long ago they gained access.

I apologize for having to warn you of this, I am taking steps to insure that our customer information remains safe. I promise to let you know of any such scams in the future, but please help me out by letting me know if you get any strange contact trying to use our relationship with you to obtain any information.

Matt Giger, Lunar Software, Inc. mgiger@lunarsoft.com

---

## **✶ Excel date munging: what a difference --four years and-- a day makes**

Tom Walker <timework@vcn.bc.ca>  
*Sun, 10 Jun 2001 07:33:20 -0700 (PDT)*

A couple of months ago I was replying to a expert-witness report in an arbitration and found that his years of service calculations were wrong by four years. Then last week I received an excel file from the other side's lawyers in the case and noticed that when I cut and paste a column of dates

they all automatically went back four years and a day. The problem arises from incompatibility between the 1904 date system used by excel in mac and the 1900 date system used in windows. This is a known and documented feature of excel:

<http://support.microsoft.com/support/kb/articles/q180/1/62.asp>

However, a quick search on the Web and in the Risks Forum archives suggests the risk isn't that widely appreciated. Even if one knows about the anomaly and checks for date system compatibility before cutting and pasting dates, one still could receive files from a source that already had corrupted dates. There would be no way of knowing (other than common sense if the results are not credible).

It seems to me that the errors introduced into spreadsheet calculations will tend to be systematic rather than random because: 1. they will often occur when two or more sets of data are being consolidated and thus the errors will apply to the population of one set but not to the other and 2. the direction of the error will be influenced by the prevalence of macs or pcs in different institutional settings and fields, e.g., macs in universities & design and pcs in businesses & finance. Thus, for example, dates systematically advance from businesses to universities and recede from design to finance. This makes collaborative work between institutions and professions especially vulnerable.

The first time (that I know of) that I encountered the problem was a

practical instance with a potentially significant economic impact on several thousand employees. The fact that the data was presented in the course of an adversarial process was probably crucial to the error having been detected.

I am wondering why there aren't more reports out there of encounters with this problem. Is this bug flying under the radar?

Tom Walker, Bowen Island, BC 1-604-947-2213

---

## **✶ Dead men produce no documentation**

"Dankmyer, Kirt" <Kirt.Dankmyer@csconline.com>

*Fri, 8 Jun 2001 14:59:11 -0500*

I was recently assigned to take over a system that processes and sends data to a wide variety of scientific agencies that depend on said data. In particular, I've been asked to understand the system well enough to maintain and troubleshoot it.

Naturally, the system, both software and hardware, was created "in-house" by contractors. Nothing like anything I'd experienced before. When I requested documentation, I was told there was none. The last person who had to work on the system had produced a draft of user documentation, but it was incomplete.

So, I contacted the poor soul who had worked on this system before me, the one who had produced the incomplete documentation. (We'll call her Joan.) Joan was only familiar with the part of the system she had

worked on (the user interface, really). So I asked her about the two people who had designed and implemented the system in the first place. I thought that they could perhaps help me with some of the questions I had.

One of them had left the company that originally employed her, and wouldn't return phone calls. So I asked Joan about the other designer, who seemed to have done the bulk of the work anyway.

"He's dead," Joan told me. "Heart attack."

The risk? If you skimp on documentation while designing a custom system, you may find that you don't have time to go back and do it later, with serious consequences for those who follow you. This problem should be familiar to most readers of RISKS, but it bears repeating. As I write this, a problem has come up with the system and no one is even sure if it is hardware or software. When dealing with such a system, you cannot guarantee you will be able to talk to the original designer (and the only one who understands the system fully), and it might be because they've left more than just the company that originally produced the equipment. Sic transit gloria mundi...

Kirt Dankmyer -- 757-824-2283 -- kirt.dankmyer@csconline.com  
CSOC UNIX System Administrator -- Wallops Flight Facility

[Of course, Wallops Island is where a lightning strike hit the missile

launch platform when a missile was waiting to be launched to test the

effects of lightning -- and resulted in the missile accidentally being

launched. PGN]

---

## REVIEW: "Inside Internet Security", Jeff Crume

Rob Slade <rslade@sprint.ca>

Mon, 11 Jun 2001 18:21:13 -0800

BKININSC.RVW 20010511

"Inside Internet Security", Jeff Crume, 2000, 0-201-67516-1, U  
\$29.95

%A Jeff Crume crume@us.ibm.com

%C P.O. Box 520, 26 Prince Andrew Place, Don Mills, Ontario  
M3C 2T8

%D 2000

%G 0-201-67516-1

%I Addison-Wesley Publishing Co.

%O U\$29.95 416-447-5101 fax: 416-443-0948 bkexpress@aw.com

%P 270 p.

%T "Inside Internet Security: What Hackers Don't Want You to  
Know"

Recently I started teaching a new class. During the introductions, one student admitted that he wanted to learn how to break into systems since that would teach him how to protect them, right? In the first place, I don't believe him. In the second, his thesis is seriously flawed. Yet that is the type of argument Crume seems to be making in the introduction to this book: learning how to hack will teach you how to protect yourself. It doesn't work that way. Knowing how to exploit a buffer overflow in Microsoft's Internet Information Server doesn't teach you anything about the type of systems development practices that will keep you from

leaving buffer  
overflow loopholes in your own programs.

Crume does, however, present some good, if basic, security advice. After a bit of a rocky start.

Chapter one says that there are weaknesses in the net. Big surprise.

Chapter two says that the Net is possibly dangerous. About the only reliable information you'll get out of chapter three is that hackers differ.

By chapter four, though, the book has settled down. Here we get a decent introduction to risk analysis, stressing that some risks are not worth protecting against. There is some solid advice about security policies in chapter five, most notably, have one.

Chapter seven lists some good general points to keep in mind, which then become the titles of the remaining chapters. There is a clear, if not terribly detailed, explanation of what firewalls are and do, in chapter eight. We are warned to be wary of insiders in chapter nine, which also points out that not all "insiders" are actually inside. Chapter ten outlines some of the aspects of social engineering. A detailed discussion of passwords, in chapter eleven, even covers tokens and biometrics. Network and packet sniffing is explained in chapter twelve. Chapter thirteen is weak. Ironically, it is the first chapter to touch closely on the items Crume implied in the introduction, and looks at software vulnerabilities.

But these loopholes are very difficult to deal with, and the

material here isn't much help. Chapter fourteen is helpful in pointing out that factory set defaults can be dangerous. The title of chapter fifteen ("it takes a thief to catch a thief") seems to be suggesting that you hire hackers. Actually, it merely suggests that you learn the vulnerabilities that they know. However, it isn't very useful in pointing the reader in the right direction. Chapter sixteen offers a grab bag of anecdotal reports of recently exploited vulnerabilities.

And, of course, I have to pay special attention to chapter seventeen, on viruses. Well, Crume makes mistakes, but he doesn't make any really important ones. The background is reasonable, and the advice is sound.

Chapter nineteen provides a good overview of cryptology, but some of the more important points get buried in the stories. (There is more material provided in appendix A.) Backdoors and end runs are discussed in chapter twenty. Chapter twenty one points out that even "harmless" defacement of a Web site can have serious consequences, while twenty two says the information is valuable and a good defence. Chapter twenty three finishes off with a look at some emerging technologies that are bringing forward new security concerns.

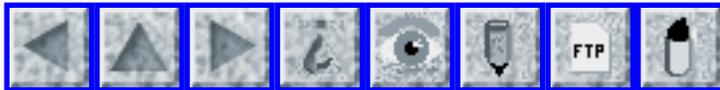
One note that I should make: the text doesn't have all that much to say about the Internet, as such. Most of the points deal with security on a general basis. Which doesn't necessarily make it any less

useful.

This book can be read completely in a day. And, for most managers and business people it would be a day very well spent. While some chapters are weak, roughly three quarters of the material is both reasonable and technically sound, a match that happens less often than one might wish. This is definitely a volume to get to pass around among all employees--and to provide to all newly hired managers.

copyright Robert M. Slade, 2001 BKININSC.RVW 20010511  
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 21: Issue 48**

**Monday 18 June 2001**

## Contents

- [Unexpected network congestion: remote consequences of Seti@Home](#)  
[Steve Loughran](#)
- [Site puts private cell calls on Web](#)  
[Bruce Hamilton](#)
- [European Commission "Net-security" site invaded by hackers](#)  
[Declan McCullagh](#)
- [Formula 1's string of control-system failures](#)  
[Stellios Keskinidis](#)
- [A320 Incident](#)  
[Peter B. Ladkin](#)
- [Re: Computer train trauma](#)  
[Philip Nasadowski](#)
- [Lincolnshire University offers first course on rail disasters](#)  
[Tom Van Vleck](#)
- [NYSE: "Throw up your hands and reboot"](#)  
[Chris Norloff](#)
- [Re: Billboard error messages](#)  
[David M Chess](#)
- [Response to LWN's statement about Linux security costs](#)  
[Kevin Postlewaite via Gerrit Muller](#)

- [Windows XP adds its own links](#)  
[George C. Kaplan](#)
  - [Re: Office XP modifies what you type](#)  
[Andy Newman](#)  
[Gerard A. Joseph](#)
  - [Re: Steve Gibson's and Windows XP](#)  
[Chris Dodd](#)
  - [Re: The risks of clueless marketing](#)  
[Tony Martin-Jones](#)
  - [Re: And you thought Keith Lynch was kidding!](#)  
[Phil Carmody](#)  
[Paul Ward](#)  
[Ken Knowlton](#)
  - [On the deceptiveness of pop-under ads](#)  
[ocschwar](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

## ⚡ Unexpected network congestion: remote consequences of Seti@Home

"Steve Loughran" <slo4@iseran.com>  
*Tue, 12 Jun 2001 17:10:24 -0700*

I came across an interesting little article on Sun's best practices site, titled, "Network Wedged by Little Green Men"  
[http://dcb.sun.com/practices/devtales/network\\_wedged.jsp](http://dcb.sun.com/practices/devtales/network_wedged.jsp)

It covers how a small firm's network kept on slowing down to a halt. The problem was tracked down to Seti@home screen savers repeatedly trying to connect to the Seti servers, which were inaccessible due to attempted cable theft (as noted in past RISKS). The local firm's Internet access used NAT

address translation, and each screen saver made multiple attempts to connect. Each connection attempt used a NAT assignment, an assignment which took a while to be cleaned up. Before long the company had exhausted their pool of 128 NAT addresses, even though only six people were present. Only through router interrogation was the problem identified.

The article closes by saying the problem was "solved" by increasing the number of available NAT addresses, although of course that didn't fix the problem, merely caused it to 'go away'. A real solution would be to have the screen-saver software implement incremental backoff and other mechanisms designed to gracefully handle a complete loss of remote server access.

One would hope that the authors of the next generation of distributed computation applications take heed of the lessons of the current batch.

-Steve

---

## **Site puts private cell calls on Web**

<bruce\_hamilton@agilent.com>  
*Thu, 7 Jun 2001 10:57:01 -0700*

Citizens in Ottawa were probably not aware that they were providing content for a new Web site that streams live audio onto the Net. The site uses conversations pulled from a radio that scans cellphone frequencies in the

city. \*CTIA Daily News\* <<http://www.canoe.ca/OttawaNews/OS.OS-06-07-0003.html>>

Bruce Hamilton bruce\_hamilton@agilent.com Tel: 650-485-2818  
Fax: 650-485-8092  
Agilent Technologies MS 24M-A, 3500 Deer Creek Road, Palo Alto  
CA 94303

---

## ✶ European Commission "Net-security" site invaded by hackers

Declan McCullagh <declan@well.com>

*Wed, 13 Jun 2001 09:58:18 -0400*

European 'safer Internet' site hit by hackers, By Joris Evers  
(IDG)

<http://www.cnn.com/2001/TECH/internet/06/11/safer.net.hack.idg/index.html>

Hackers embarrassed the European Commission last week by identifying and exploiting two security holes on a new commission-sponsored Web site that promotes safer use of the Internet. One of the holes allowed the hackers to get administrator privileges on the server that powers the Safer Internet Exchange site [...]

---

## ✶ Formula 1's string of control-system failures

Stellios Keskinidis <stelliosk@optushome.com.au>

*Fri, 8 Jun 2001 18:35:48 +1000 (EST)*

If you've been watching F1 over the past month or so you would of very likely heard about making launch control and traction control systems legal and how nearly all teams are using them. Unfortunately, not all things have been going to plan for team I am the most a fan of -

"Since the electronic device was legalised by the FIA at the Spanish Grand Prix, Mika Hakkinen has fallen foul of it once and Coulthard twice. Software programming has been stated as being the main cause of its malfunction."

- <http://www.formula1.com/news/headlines01/06/s5819.html>

and further

"Coulthard stalled his car on the grid at the first traction control race in Barcelona prompting team boss Ron Dennis (Team Boss), to accuse him of 'Brain fade'.... Dennis admitted that it was a software glitch and he was wrong to have thought that it may have been down to driver error. "

- <http://www.formula1.com/news/headlines01/05/s5731.html>

not to mention the four cars that stalled it on the grid in Austria

"Several teams have expressed their anxiety over the possibility of a recurrence of the situation in Austria, where four cars failed to start. With the narrowness of the makeshift pit straight on the Monte Carlo street circuit there will be less room in which to manoeuvre cars and avoid potential disaster."

- <http://www.formula1.com/news/headlines01/05/s5607.html>

Are the cars becoming too computerised and resulting in more points of failure? Are the teams throwing themselves out of the competition by not testing properly, possibly due to the time constraints? The catch there is that they think they are ready (in testing) when they are not in a live run paying a costly price. Just another classic case of Software Engineering.

Cars can only go so fast around any track, I think within the next 5-10 years they will reach their limits in speed and the teams will focus more than they are now, on the "computerisation" of the car where we will see more failures/crashes and stalls on the grid.

This sounds all too familiar when the aviation industry embraced technology. Are they repeating those mistakes? It can now be said "Would you hop into a car that travels over 300km/h that is controlled by software you wrote".

One thing is for sure, this is soon to be race against technology and not who was the better driver on the day and as if it wasn't already a 2-man race anyway (McLaren and Ferrari).

Stellios Keskinidis <http://members.optushome.com.au/stelliosk>

---

## **A320 Incident**

"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>

*Mon, 18 Jun 2001 12:54:17 +0200*

Tim van Beveren reported in *\*Flight International\**, 22-28 May 2001, on a 20 Mar 2001 incident to a Lufthansa Airbus A320 on takeoff from Frankfurt.

This incident was reported at greater length and detail in *\*Air Safety Week\**, 4 Jun 2001, by David Evans and Tim van Beveren.

The captain was Pilot Flying (PF). there was some degree of turbulence during takeoff, shortly after rotation, which resulted in the left wing moving down. The captain applied correction (right lateral roll control) but the wing dipped further left, reaching 21 degrees bank, and the wingtip is reported to have come within half a meter of the ground, and according to computer modelling of the digital flight data recorder the airplane "came within a few seconds of striking the ground".

The First Officer, the pilot not flying (PNF), realising there could be a control problem, switched "priority" to his sidestick controller and recovered the aircraft. The aircraft was flown up to 12,000ft on autopilot, the crew confirmed the problem, that the CAP's sidestick was controlling for roll in the reverse sense (normally, putting the sidestick to the left commands left roll; to the right commands right roll. Control-reversal here means that CAP's sidestick gave right roll on a left movement and left roll on a right movement).

The aircraft had just come out of maintenance. Maintenance is a

known risk --

James Reason, an authority on human factors in aviation safety and Professor of Psychology at the University of Manchester, amongst others, has detailed how significant problems may arise through maintenance of complex systems.

It has happened many times that aircraft have come out of maintenance with control systems reversed in one or more of the three axes (roll, pitch, yaw). This has been the cause of a number of accidents with general aviation aircraft, but my informal requests for information turned up no recent accidents to commercial aircraft due to this cause. Evans and van Beveren report that "reversed controls are deemed impossible on transport-category aircraft" and that Boeing claims that the B737 aircraft cannot be reverse-connected without it being discovered before flight, normally through mandatory post-maintenance checks, but at the latest by the pilot's preflight check, as the controls could not be moved.

At Lufthansa's code-sharing partner, United Air Lines, certified inspectors must be stationed both inside and outside the cockpit to conduct a functional check after the flight control system has been worked on; a flight test is also required before the aircraft is returned to service after this kind of repair. It is believed that either of these measures would have caught the control-reversal problem, and so general maintenance procedures at Lufthansa Technik will be subject to detailed inquiry.

There have been a number of reports as to what fault caused the

lateral control reversal, including the two sources above. However, I have found none of the explanations so far satisfactory, as they raise further puzzles that they do not solve.

The following architectural description of the A320 primary flight control system (PFCS) is drawn from Cary R. Spitzer, Digital Avionics Systems, Second Edition, McGraw-Hill 1993. The A320 sidestick controller generates input to five of the seven flight control computers which form part of the primary flight control system (PFCS). These five are the two Elevator Aileron Computers (ELACs) and the three Spoiler Elevator Computers (SECs). Each wing has two outboard ailerons, and five inboard spoilers (overwing surfaces which can be raised). Lateral (roll) control proceeds via four of the five spoilers and the two ailerons. Each of the two ELACS and three SECs control some combination of these 12 control surfaces. There is a significant amount of control redundancy.

Initial reports said that Lufthansa Technik personnel had been repairing one of the two ELACs, and had found a damaged pin on a connector. They had replaced the connector and this had apparently caused the control reversal. This explanation made no sense to me as it stood, because

- (a) the connectors are standardised. Replacing one with another should give exactly the same connections as were there before;
- (b) if one ELAC was receiving reversed signals, and the other was not, and the three SECs were not, then
  - (i) the PFCS architecture would detect a discrepancy on the

channels, and

(ii) on each side, one aileron would operate counter to the other, but

all spoilers would operate correctly-sensed, and it is hard to see

how this could lead to the extreme control discrepancy reportedly

experienced by the PF.

The Aviation Safety Week report on June 4 suggested that "Repair work

involving complete rewiring "upstream" of the connector pins was conducted

over several work shifts". The ELAC connector with the damaged pin has 140

pins and is one of four such for the ELAC, for a total of 560 pins.

It seems to me that to get control reversal without the phenomena in (b)

above, there must have been a reversed signal downstream of the sidestick

but upstream of where the sidestick movement is multiplexed into the five

input signals to the five PFCS computers which receive them. I do not yet

have, nor have I heard, a coherent suggestion as to how that could occur.

There has been considerable discussion of and speculation concerning:

maintenance procedures at Lufthansa Technik, which has one of the very

highest reputations for maintenance quality; wiring, wiring conventions and

connectors in the A320 series; why the pilots did not discover the

discrepancy during the usual preflight control checks (the A320 displays

control surface displacement on the cockpit display, the ECAM, when the

sidestick is intentionally moved and the airplane is on the ground, as

during a preflight control system check). I think it is fair to say that few hard facts have emerged yet concerning any of these, and I find it hard to make any useful inferences about what actually went on from the publicly available information.

What emerges most clearly so far from this incident is that the simple physical complexity of the control system has confused some. Amongst other things, explanations have been proposed by presumably technically competent people that do not fit the control system architecture. It is hard to see how that phenomenon could have occurred with the simpler architectures of mechanical control systems. On the other hand, the PNF was able to take over normal control of the aircraft with one button push (the "control priority" takeover on the sidestick), which could also not happen with the simpler mechanical architectures.

We have very little information so far on the incident. It is certain that the puzzles will be solved further along the investigative line, and very likely that the results of the investigation will be highly significant for the care and feeding of fly-by-wire architectures.

Peter Ladkin, University of Bielefeld, <http://www.rvs.uni-bielefeld.de>

---

**⚡ Re: Computer train trauma ([RISKS-21.47](#))**

Philip Nasadowski <nasadowsk@mail.hartford.edu>

Sat, 16 Jun 2001 21:45:17 -0400

[PGN notes: Lord Wodehouse forwarded Philip's reply to his message

in [RISKS-21.47](#), with this comment:

As we make systems more complex and clever, they become when they fail,

less reliable and more stupid. The present efforts to overcomplicate engineering solutions in the name of progress and efficiency thus

continues the themes explored in Edward Tenner's book Why Things Bite

Back published 1996, which although I do not like his term "revenge

effect", because it is too emotive, is a good description of various

well intentioned(?) ideas and efforts that have had surprising(?)

results, which were not what was intended. Pharmaceutical companies not

excepted either! John]

I'm in the US, and we have the same stupidity over here too.

The new GE

locomotives for Amtrak (our national joke of a railroad) are excessively

computerized, and grind to a halt on occasion - requiring a lengthy (10

minutes!) reboot. This is especially bad when one dies on approach to NY

city!

The recent Long Island Rail Road cars have had numerous problems too: The

automated announcements are always not working (to the extent of announcing

stations in an order that cannot exist), worse, the computerized door

systems were an early nightmare - they would sometimes open the doors

enroute (imagine a standing room only train going 60 - 80 mph over rough track), or refuse to open the doors when stopped. The latter was caused because the system will "lock out" any door panel where the conductor (guard) presses a door open/close button repeatedly (which was needed with the old pneumatic system on the old cars).

Most disturbing was the early brake failures. The computer-controlled braking systems would on occasion react very slowly to braking commands. This caused a number of trains to be removed from service, enroute.

Oddly enough, the 30 year old electric units the LIRR has, which have been battered and poorly maintained, seem to run just fine without all this computer stuff in them.

---

## **⚡ Lincolnshire University offers first course on rail disasters**

Tom Van Vleck <thvv@multicians.org>

*Mon, 18 Jun 2001 12:03:50 -0400*

[http://dailynews.yahoo.com/h/nm/20010618/od/college\\_dc\\_1.html](http://dailynews.yahoo.com/h/nm/20010618/od/college_dc_1.html)

---

## **⚡ NYSE: "Throw up your hands and reboot"**

"Chris Norloff" <cnorloff@norloff.com>

*Thu, 14 Jun 2001 08:11:00 -0400*

When the New York Stock Exchange computer systems crashed for 85 minutes (8 Jun 2001), Andrew Brooks, chief of equity trading at Baltimore mutual fund giant T. Rowe Price, was quoted as saying "Hey, we're all subject to the vagaries of technology. It happens on your own PC at home. You just throw up your hands and reboot."

The RISKS?

Thinking that a world trading center needs no more reliability than a desktop PC.

A certain company (who's "not a monopoly") is training legions of users to expect computer systems to be unreliable.

source:

<http://www.washingtonpost.com/ac3/ContentServer?articleid=A42885-2001Jun8&pagename=article>

Chris Norloff

---

## ⚡ Re: Billboard error messages ([RISKS-21.45,46](#))

"David M Chess" <chess@us.ibm.com>

Wed, 13 Jun 2001 16:53:44 -0400

The most notable example I've seen was one of those portable highway-side signs that was declaring in foot-high letters "BATTERIES NEED RECHARGING".

I suffered momentary brain-lock trying to figure out how it could know that

some car going by had a battery problem.

The general risk, of course, is in piping STDERR to STDOUT. Web sites that send complex error dumps to visitors' browsers are doing the same pointless thing...

---

## ✶ Response to LWN's statement about Linux security costs

"Kevin Postlewaite" <kevin.postlewaite@tumbleweed.com>

Date: Thu, 31 May 2001 12:25:25 -0700

[From Linux Weekly News, courtesy of Gerrit Muller, Re:  
<http://www.extra.research.philips.com/natlab/sysarch/>]

In LWN's front page article about the relative security costs of Linux

versus Windows, you wrote:

"While it is nice to see a (hopefully) objective result that favors Linux,

it is also a little disappointing. 5-15% is a fairly small margin; we

should really be able to do better than that. It's a start, anyway. "

I used to work for PricewaterhouseCoopers auditing computer security of our clients. We would go in and try to penetrate our clients' systems (with their permission, of course). The main flaws that existed did not have to do with the particular OS but depended on the skill and conscientiousness of the system administrators, as well as the computer-security education of the company's employees. The most successful penetrations were obtained when

some sysadmin would set the root password to root (or better yet, none at all) or have the Windows Administrator password be Administrator. Also, a surprisingly high number of employees would gladly give out useful information (including accounts and passwords) to people that they didn't know over the phone. People were the weakest link, not the OSes. Thus, I wouldn't expect that the underlying OS would affect the expected damages by much. Far more important than installing Linux is educating the users(not that they shouldn't install Linux anyway :- ) ).

-Kevin

---

## ✶ Windows XP adds its own links

"George C. Kaplan" <gckaplan@ack.Berkeley.EDU>

*Thu, 07 Jun 2001 20:37:04 -0700*

Walter S. Mossberg's "Personal Technology" (\*Wall Street Journal\*, 7 Jun 2001) describes a new "feature" of Internet Explorer under Windows XP: it will turn some words on web pages you view into hyperlinks, pointing to Microsoft web sites.

So, first we have Office XP changing your documents as you type them, without telling you (Jonathan Arnold, [RISKS-21.42](#)). Now Internet Explorer will edit your documents for you at the other end: when people read them.

Mossberg discusses this feature and the associated risks in

detail.

Microsoft's arrogance shines through brilliantly in one quote:  
the new  
feature "will spare users from 'under-linked' sites".

Words fail me.

George C. Kaplan, Communication & Network Services  
University of California at Berkeley 510-643-0496 gckaplan@ack.  
berkeley.edu

---

## **⚡ Re: Office XP modifies what you type (Deegan/Arnold, [RISKS-21.42](#))**

Andy Newman <andy@silverbrook.com.au>

*Thu, 14 Jun 2001 08:42:32 +1000*

Thanks to the many who pointed out my mis-reading of the RFC and the missing  
of the empty path segment. Therefore MS *\*are\** wrong in  
modifying the path.

The interesting thing is I fell into the risk I pointed out -  
seeing a  
collection of '/' separated tokens (empty or not) made me apply  
a file  
system interpretation to a URL and stopped me even contemplating  
what use an  
empty path component is and why it should be valid.

Andy Newman, Silverbrook Research, <andy@silverbrook.com.au>

---

## **⚡ Re: Office XP modifies what you type (Deegan/Arnold, [RISKS-21.42](#))**

"Gerard A. Joseph" <gerard@ozemail.com.au>

Wed, 13 Jun 2001 17:05:56 +1000

I am in total agreement with the people complaining about automatically-enabled mechanisms that unilaterally correct textual input.

I have just migrated to Windows 2000 and am now in a state of euphoria that

I can actually enter a one-word folder name in upper case without the second

and subsequent letters being preemptively and irreversibly changed to lower

case. Imagine, I can now name a folder NSA without it reappearing as Nsa.

(If it was possible to do this in Windows 95, no one was able to tell me how.)

For years, I have had to put up with such aberrations as letters addressed

to "Mr Ga Joseph", a combination of an autocorrect feature that is enabled

by default (or by an administrator), and an imbecilic writer who (a) omits

periods between initials, (b) doesn't know how to either turn off the

feature or reverse its individual perpetrations, (c) accepts as gospel

anything the word processor dishes up from his input, and (d) lacks the

intelligence or good manners to care about any of the foregoing. And then

all those well-known organizations Ibm, Cia, Hr, Po, Cert, Un, etc.

Of course, at the spiritual heart of all this nonsense is the bone-headed

spelling checker, one of the stupidest abominations ever unleashed on a

para-literate user community.

There's a universal truth, as true in textual composition as it is in computer security: no piece of technology can substitute for appropriate human practices.

---

**✉ Re: Steve Gibson's and Windows XP (Crooke, [RISKS-21.46](#))**

Chris Dodd <chrisd@reservoir.com>

*Fri, 15 Jun 2001 06:19:25 -0000*

> It is also time for backbone providers to introduce sensible firebreaks  
> and reduce their trust in traffic passing through their systems.

IMO this conclusion is completely wrong -- the whole point of the Internet is that the component parts need not be trusted to be infallible. Its never been the case that the endpoints are entirely trustworthy, but as the Internet grows, this problem becomes more noticeable. As far as the proposed solution is concerned, its already the case that potentially useful features of the Internet (such as source routing) are mostly useless due to the fact that many routers don't follow the protocol in the name of security. Source IP filtering (at least as proposed by RFC 2827) is even worse, as it breaks things that are actually being used, such as Mobile IP (RFC 2002). What's more, it wouldn't even do anything to stop the attack reported by Steve.

The real RISK here is in the rush to improve security (at least for some people), we end up seriously impairing the functionality of the Internet for everyone.

Chris Dodd <chrisd@reservoir.com>

---

## ⚡ Re: The risks of clueless marketing (J.McCarthy [RISKS-21.46](#))

Tony Martin-Jones <tmj@enternet.com.au>

*Thu, 14 Jun 2001 06:48:09 +1000 (EST)*

On the contrary: as "XP" are the Greek letters of the chi-rho, the monogram for the name of Christ, they obviously hope it will be Micros\*\*t's saviour.

---

## ⚡ Re: And you thought Keith Lynch was kidding! ([RISKS-21.47](#))

Phil Carmody <fatphil\_without\_this\_suffix@altavista.com>

*Thu, 14 Jun 2001 17:31:03 GMT*

It's not really the 'HEX' that is the gz file, it's the 'binary', written in LSB-last format (and the LSB is byte-aligned). For reference, it is not the whole of the source that has been zipped, as that was too large to mathematically prove as prime -- it is just the descramble functions. My justification was that copyleft's 2 T-shirts did the same split, and they were subpoenaed for them both. No attempt was made to be clever,

I simply  
wanted source code that had been already accused of being a  
circumvention  
device to be propagated.

[My favourite headline was "When Mathematicians Turn Bad", in  
\*The Register\*.]

Phil

[Phil noted subsequently that Keith's posting was two months  
after

Phil's earlier postings, and that RISKS is actually  
recycling a topic

that has been beaten to death elsewhere. Apologies to  
readers of

elsewhere. PGN]

---

## **⚡ Re: And you thought Keith Lynch was kidding! (PGN, [RISKS-21.42](#))**

<pasward@styx.uwaterloo.ca>

*14 Jun 2001 10:28:43 -0400*

One of the strangest consequences of copyright law is that it  
would seem to  
outlaw possession of certain integers, as does trademark and  
trade secret  
law. In fact, any piece of intellectual property can be encoded  
as a single  
integer, which would be protected. Don't blame DMCA for what is  
an inherent  
property of all intellectual property law.

paulward (DrGS)

---

## **⚡ Re: And you thought Keith Lynch was kidding!**

<KCKnowlton@aol.com>

*Wed, 13 Jun 2001 21:11:32 EDT*

Illegal possession of certain integers ([RISKS Vol 21 Issue 47](#)) is not really new. Any 10-color, 200x200-pixel image of child pornography is simply a 40,000-digit integer that I think, for quite some time now, has been illegal for you to possess.

Ken Knowlton

---

## **⚡ On the deceptiveness of pop-under ads (Re: [RISKS-21.47](#))**

"The guy named after an Om Kalthoum song" <ocschwar@MIT.EDU>

*Thu, 14 Jun 2001 03:55:13 -0400*

Nytimes.com and latimes.com do indeed use pop-unders, but if you look at the script used to pop them, you will find that in the NY Times version, there is a myDelay variable, but it is set to 0, and no such variable in the LA Times version.

The folks in fastclick.net ought to kick themselves for even thinking of delaying the pop-unders, without which their ethics would be less likely to fall under criticism. The folks in nytimes.com deserve both credit and discredit for setting myDelay to 0. Of course, this still leaves them open

to reprobation if someone visits their site while his computer is under a heavy load, and the pop-under takes a while to pop under.

Pop-unders, when their origin isn't concealed, are actually a smart idea.

One of the problems with web advertising for funding the Web is that under that scheme writers attract viewers only to send them to who-knows-where.

This solves that problem by attracting the viewer to the ad after he is done reading the article and thus more likely to have a look-see.

And the RISK? There is no need to compromise your own reputation by writing the equivalent of this:  
" \$I\_Am\_Slimy = 0; if (\$I\_Am\_Slimy) { ... }" when you can just choose not to be slimy.



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 21: Issue 49**

**Monday 18 June 2001**

## Contents

- [Passive radar? Removing the cloak of invisibility](#)  
[What's New via Dave Farber](#)
- [Therac Returns: Data-entry errors kill five patients in Panama](#)  
[Allan Noordvyk](#)
- [WashingtonPost.com real estate database](#)  
[Nick Laflamme](#)
- [ebates.com installs Java program on users computer](#)  
[Bill Tolle](#)
- [Risks of peer-to-peer in the office](#)  
[Alpha Lau](#)
- [PCs used as cash registers](#)  
[Nick Brown](#)
- [Software "worm" searches your computer for pornography](#)  
[NewsScan](#)
- [Conflicting sensors placed on different parts of the line](#)  
[Robert Gordon](#)
- [New world disorder?](#)  
[Mike Coleman](#)
- [Security vulnerability databases](#)  
[Uwe Ohse](#)

- [Yet another e-commerce error](#)  
[Leonard Erickson](#)
  - [Re: PC parrot: telephone bird vs. real phone ring](#)  
[Dan Jacobson](#)
  - [Re: Banning virtual forms of entertainment \(](#)  
[Gerard A. Joseph](#)
  - [Re: Formula 1's string of ... failures](#)  
[Bob Dubery](#)  
[Chris Kantarjiev](#)
  - [The magic, fast-food, wand](#)  
[Rob Slade](#)
  - [QWE2001: Call for Papers and Presentations](#)  
[SR/Institute](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

## ✶ Passive radar? Removing the cloak of invisibility (What's New)

David Farber <dave@farber.net>

Sat, 16 Jun 2001 10:39:31 -0400

So just how stealthy is the \$3.6B stealth bomber? Radar would need to look straight up at the bomber's flat bottom surface. Tracking would therefore require a vast array of antennas. But according to a story early this week in the \*London Daily Telegraph\*, such arrays already exist: Roke Manor Research in Britain claims that stealth aircraft can be tracked by their effect on ordinary mobile phone traffic. News media in the US did not discover the story until last night. The Pentagon is taking it seriously, and other nations, including China, are now developing such a system.

[Source: What's New, 15 Jun 2001, from Dave Farber's IP

distribution]

---

## ✶ Therac Returns: Data-entry errors kill five patients in Panama

"Allan Noordvyk" <noordvyk@home.com>

Sat, 16 Jun 2001 06:50:03 -0700

>From the \*Seattle Times\*:

... data entered incorrectly in a computer program used in radiation

therapy for cancer patients has caused at least five deaths in Panama ...

For 28 cancer patients, healthy tissue was inadvertently exposed to high

levels of radiation, David Kyd, spokesman for the International Atomic

Energy Agency, said yesterday. So far, five deaths have been linked to the

radiation exposure, while two other deaths are from "ambiguous" causes, he

said. One patient died from cancer. Agency experts expect two-thirds of

the surviving patients to develop serious complications.

Radiologists

using the program assumed the computer software had a fail-safe mechanism

that would prevent healthy tissue from being exposed to radiation, Kyd

said. But the five radiology experts from the International Atomic Energy

Agency found health-care workers incorrectly entered the data, administering dangerous levels of radiation to healthy tissue. Kyd said,

"had the instruction manual been followed to the letter, this wouldn't

have happened. But this wasn't done."

Full text of the article can be found at:

<http://archives.seattletimes.nwsourc.com/cgi-bin/teaxis/web/vortex/display?slug=radiation14&date=20010614>

[PGN Note: Therac background in [RISKS-9.20](#), [RISKS-14.04](#), [RISKS-14.75](#), and [http://courses.cs.vt.edu/~cs3604/lib/Therac\\_25/Therac\\_1.html](http://courses.cs.vt.edu/~cs3604/lib/Therac_25/Therac_1.html)]

Allan Noordvyk, Software Artisan

[Added later: The company has issued a response, at: <http://www.multidata-systems.com/PDFs/MDresponse.PDF>]

---

## WashingtonPost.com real estate database

Nick Laflamme <[dplaflamme@alumni.nd.edu](mailto:dplaflamme@alumni.nd.edu)>  
*Thu, 14 Jun 2001 10:20:26 -0400*

WashingtonPost.com, in association with a local real estate agency, has put up a database of home sale prices and property tax appraisal values.

They've merged together tax records and real estate deed updates from several counties in the Washington, DC, metropolitan area, and some of the records are as detailed as any Multiple Listing Service listing you'd find while looking for a home to buy.

This data base will prove useful for people trying to compare the price of a property they're considering with the values of the neighboring properties. However, because you can search by owner as well as by zip code or address, it has some nasty privacy implications. For instance, I can

find the listing on my former manager's home knowing only his last name and the county in which he lives. Worse, I can find his street address, something not available to me through conventional sources.

Trolling through deed listings and the like is an old risk. Consolidating it and putting a too easy to use Web interface on it is a comparatively new risk.

Inquiries to washingtonpost.com about the privacy implications of this were referred to their Real Estate editor, who has not responded after more than a week.

It's enough to make me even more glad that I rent, not own, my home.

Nick Laflamme, Vienna, VA

---

## **ebates.com installs Java program on users computer**

Bill Tolle <BillTolle@ExclusiveBuyersAgents.com>

*Fri, 15 Jun 2001 09:51:20 -0500*

Being a frequent shopper on the Internet I "bit" on an offer from <http://www.ebates.com>. They offer a rebated from merchants if you go through ebates.com to get to the merchants site. I made the mistake of assuming that Buy.com and BarnesandNoble.com would not associate themselves with anything illegitimate. That was a mistake.

I read ebates.com's privacy policy and the only thing it mentions is

"cookies", not a word about any other type of tracking software.

My second mistake was that I had enable Java in Internet Explorer while trying to solve some problems and had failed to disable it later.

I signed up for their service. Later that same day, after I had rebooted my computer I found that a program named "Javarun.exe" was trying to access the Internet and was also trying to act as a server for the Internet. Fortunately, the firewall caught it and stopped it.

Upon investigation, I found that ebates had installed a new folder named "C:\Program Files\topmoxie" that included the Javarun.exe program. There was also a file named "einstall.txt" in the C:\ directory that shows the installation of 134 ".class", ".dll", etc. files.

Fortunately I had backed up my registry earlier in the day and was able to restore it to a point before I signed up with ebates. I am waiting for a reply from Buy.com and BarnesandNoble.com regarding my complaints to them for being associated with such an illegitimate operation as this.

Bill Tolle, 245 S. Peachtree St., Jasper, Texas 75951  
1-866-378-8525 - (409) 384-9094 <http://ExclusiveBuyersAgents.com>

---

## ⚡ Risks of peer-to-peer in the office

Alpha Lau <avlxyz@yahoo.com>  
*Wed, 13 Jun 2001 17:17:31 +0100 (BST)*

A new line of business software introduced [12 Jun 2001] by

AltaVista will

let workers scour corporate networks, e-mail accounts and personal

computers by stitching together valuable and sometimes embarrassing

information scattered on far-flung office systems. ...

By making it easy to retrieve information from a hodgepodge of computer

servers, e-mail accounts and PC hard drives, the search software

effectively creates a peer-to-peer network similar to the one popularized

by the online music-sharing Web site Napster, which is battling to stay

afloat after running afoul of copyright laws.

The AltaVista software is based on the premise that businesses operating

in an information-driven era will be better off if more employees can sift

through a community storehouse of data gathered from corporate intranets,

workers' e-mail boxes and PC hard drives.

<http://www.wired.com/news/business/0,1367,44461,00.html>

The premise only holds if the network is trustable. I'm sure most of us

treat Web pages with an appropriate degree of mistrust.

As for Napster, How many MP3s downloaded are actually of good quality?!

I wonder how many pointy haired bosses would fall for a document posted on a

server with no links to it, but submitted to the master index...

Not to mention the privacy risks stated in the article...

---

## PCs used as cash registers

BROWN Nick <Nick.BROWN@coe.int>

*Fri, 15 Jun 2001 15:40:24 +0200*

I had an illuminating experience today while waiting in line to pay at a sports shop. The clerk/cashier at the register next to where I was waiting finished her shift and was replaced by a colleague, so I got to see how the changeover worked. And for once, although it involves Microsoft products, this is not really an MS-bashing story, but just another tale of complacency and idiocy from corporate IT.

I had already noticed the small (and very cute) LCD display (10 inch TFT, perhaps), but the first indication I had of the fun to come was when the first cashier stood up and the Windows NT logon prompt appeared as her logoff completed. The second cashier then sat down and typed her username and her password (which appeared to consist of two letters...).

I was then surprised to see four "DOS windows" (Microsoft has another name for these, but you know what I mean) pop open and display various messages, as a whole series of programs started up. Most notable among these was a virus checker. It seemed to be taking some time to complete, and although NT had not been setup to prevent the desktop loading until the check was complete, the user decided to clear it from her screen anyway. Instead of minimising it, she killed it (and the three other DOS windows) with the "X" button.

Some preliminary conclusions (that old oxymoron again):

- The register is using basic NT logon procedures (with a trivial password) as some form of "security".
- They have installed some el-cheapo anti-virus software which \*doesn't run in the background\*.
- The users are killing the anti-virus software, either because it slows down their work, or because they haven't had the minimum training required to know how to minimise a window. (Of course, the window could have been started minimised anyway.)
- Since the PC has no diskette drive or Internet connection (I asked), it's not even clear exactly what virus threat is being protected against. Or when the A-V software was last updated...

Overall summary: this company's IT department is staffed by people who have no understanding of the issues, just a boss who demands buzzword-based "results". I'd hazard a guess that they are patting themselves on the back because their anti-virus software has successfully kept out (as in, not detected any) viruses !

PS: I suppose it's superfluous to mention that the large monitor above the entrance to the store, which is meant to display the store's Web page, has, on the last three occasions I've visited, displayed a blue screen of death... from Windows 9x, not even NT.

## ✦ Software "worm" searches your computer for pornography

"NewsScan" <newsscan@newsscan.com>

*Mon, 11 Jun 2001 08:47:20 -0700*

A new computer virus called VBS.Noped.a now circulating invades computer memories in a hunt for picture files with pornographic-sounding names and reports them to the police. The virus (a "worm") arrives from an unknown source as an e-mail attachment with the subject line: "FWD: Help us ALL to END ILLEGAL child porn NOW." If it finds suspected pornography, it sends a message to the police saying: "This is Antipedo2001. I have found a PC with known child pornography files on the hard drive. I have included a listing below and included a sample for your convenience." An executive of the National Center for Missing and Exploited Children has repudiated the rogue effort and says his group "does not support unlawful means even to achieve meritorious ends." [\*The New York Times\*, 11 Jun 2001; NewsScan Daily, 11 Jun 2001; <http://www.nytimes.com/2001/06/11/technology/11VIRU.html>]

---

## ✦ Conflicting sensors placed on different parts of the line

Robert Gordon <robertwgordon@totalise.co.uk>

*Wed, 13 Jun 2001 11:05:36 +0100*

Conflicting sensors could cause power failure. In our new building, a potential design fault has come to our notice. The details are that the sensor for the load-shedding system and the sensor for starting the UPS generators are at different places upon the inward power cable. As such if the inward power feed is broken between the two sensors, the UPS will attempt to start, but the load shedding system will see no loss of power and so will not shed any noncritical systems. This could potentially cause an overload of the UPS generators whilst it is starting up and a complete failure of power to the building.

If anybody has any other new premises and datacentre risks, I would be most interested to hear what they are. I can be contacted at [robertwgordon@totalise.co.uk](mailto:robertwgordon@totalise.co.uk) Many Thanks in advance

Robert Gordon

---

## 🔥 New world disorder?

Mike Coleman <[mkc@mathdogs.com](mailto:mkc@mathdogs.com)>

*Fri, 15 Jun 2001 16:57:07 -0500 (CDT)*

In a recent `gnu.misc.discuss` thread, Florian Weimer points out that with the new locale (`il8n`) stuff, the pattern `'[A-Z]'` might also match the lowercase letters `'a'` through `'y'` (and not `'z'`, yes), depending on the setting of the `LC_COLLATE` environment variable.

(It turns out that on a current Debian Linux system, at least,

it also depends  
on whether or not the 'locale-gen' program has ever been run.)

It's not hard to imagine a slew of bugs and root exploits based  
on this  
"feature".

Mike Coleman, mkc@mathdogs.com <http://www.mathdogs.com>

---

## **✶ Security vulnerability databases**

Uwe Ohse <uwe@ohse.de>

*Wed, 13 Jun 2001 15:29:13 +0000*

I recently posted to a software security mailing list about a  
vulnerability  
in some software package.

Now I got e-mail stating someone saw an article in  
"SecurityFocus.com's  
Vulnerability Database" claiming I posted it to another security  
mailing  
list. I had a look ... and found a number of errors in the  
database entry.  
The vulnerability in question is a local one, not a remotely  
exploitable  
bug. The bug database got it exactly the other way round. The  
database entry  
states the bug exists in version 1.0, but not in 1.0.1 to .3.  
This is wrong  
- the bug exists in version 1.1.0 (i don't know about older  
versions). There  
are other minor incorrect informations.

The risk is obvious.

See <http://www.ohse.de/uwe/articles/fcron-1.1.0.html> for more  
information.

## **⚡ Yet another e-commerce error**

Leonard Erickson <shadow@krypton.rain.com>

*Fri, 8 Jun 2001 22:17:49 PST*

I'd just found a Web site offering a part I needed for an obsolete computer  
I'm working on.

I clicked the "check out" icon. I was then presented with field to enter a customer name and account number, and a button to click if I wanted to purchase without establishing an account.

I clicked the button and was presented with a screen to enter shipping address and billing address. Complete with phone number, email address, the works.

Which would have been perfectly fine, except the data for the \*last\* customer was still there.

The risks are obvious.

I assume a script error of some sort failed to clear a temporary file or buffer.

This wasn't the only error. The billing address half of the page was headed "Billing address (if different from shipping address)". But when I tried to clear out the fields, upon clicking to continue it made me go back and fill them out anyway...

And then the final insult. The item was on sale, and the price displayed was the regular price. <sigh>

I've notified the site owner and they've said they'll fix it.

The real irony is that they have a \*prominent\* notice about their privacy policy.

Leonard Erickson (aka shadow{G}) shadow@krypton.rain.com

---

## ⚡ Re: PC parrot: telephone bird vs. real phone ring ([RISKS-21.47](#))

<Dan Jacobson>

*15 Jun 2001 12:21:05 +0800*

Several times a day the Telephone Bird fools me into almost answering my cordless phone that I carry around my semi-tropical hilltop, as they sound the same. I have not identified exactly which of the many birds here makes the same sound as the phone yet.

Obviously the designers never thought that using those "neat sounds from nature" might cause problems when taken out of the expected office environment and put back into the environment they came from.

Good thing I have not installed the chirpy doorbell.

<http://www.geocities.com/jidanni> Tel1886-4-25854780 e-mail: restore .com.

[Wait until you get a voice activated computer! PGN]

**✉ Re: Banning virtual forms of entertainment (Dinwiddie, [RISKS-21.47](#))**

"Gerard A. Joseph" <gerard@ozemail.com.au>  
*Sat, 16 Jun 2001 14:36:20 +1000*

Perhaps more significantly, how do you ascertain the virtuality of something? Is the Dutch government awake to the potential difficulty of proving something is real rather than virtual?

Gerard A. Joseph

---

**✉ Re: Formula 1's string of ... failures (Keskinidis, [RISKS-21.48](#))**

"Bob Dubery" <bdubery@netcare.co.za>  
*Mon, 18 Jun 2001 22:01:02 +0200*

Things are only going to get worse.

The systems that Stellios reports on are all tied into the engine's control module and all seek to curb a limit on wheel spin, to perfectly synchronise gear changes (the gearshift also being computerised - though usually the driver can override this feature) and to generally provide optimum traction in any circumstances - usually by modulating or momentarily cutting the engine output.

These systems were banned at the end of the 1993 season, but in

reality it is impossible for the stewards to figure out who has got what in their control system and whether or not it is legal. Last year FIA (who run F1 in terms of drafting the rules and regulations) stated that a team had cheated in 1999 and would be exposed. We're still waiting, because FIA could not make their charge stick and so declined to name the offending party - even though an ex-driver had tipped them off that there was something illegal about the un-named team's cars.

So the systems are once again allowed. And they have not proven reliable (remember that each team must contrive it's own solution and so each team must write it's own software - there is no public domain code here).

As a quid pro quo for the re-admittance of systems they don't really approve of (because they take over functions that should be left to the driver), FIA have got a promise from the teams that starting 2002 the cars will be equipped with a system that will allow the stewards to impose a speed limit, apply this limit to part or all of the circuit, and force the cars to travel at this limit. Another feature to be added is a proximity detector that will (in theory) reduce the chance of collisions in wet conditions (when the cars generate huge amounts of spray).

Monaco is the narrowest circuit that F1 visits. At the start this year 4 cars were left standing on the grid because of software bugs. This left the marshalls less than a minute and a half to clear these cars out

of the way  
before 18 racing vehicles came accelerating back along the main  
straight,  
heading straight for the stationary vehicles and the marshalls.

Software that was supposed to make it easier for the drivers to  
make a good  
start has had the reverse effect. Things are now worse than when  
the driver  
had to control 850 horse power with the accelerator pedal.

At this rate of progress, and at this level of reliability, the  
so-called  
safety features could result in carnage. Picture the scene at a  
fast track  
like Spa (Belgium), Monza (Italy) or Silverstone (England) when  
the stewards  
try to reduce the cars to 80 or 90 mph because of an accident,  
and some  
car's software doesn't react, and the driver comes round a  
corner at 150 mph  
and finds slow moving vehicles, possibly an ambulance, in his  
way.

Double Risk here...

(1) These smart systems become impossible to police (in Champ  
Cars they have  
a similar problem this year, several teams are "known" to be  
cheating but  
nobody can actually prove anything)

(2) These systems could actually make things more dangerous when  
they fail.

---

**⚡ Re: Formula 1's string of ... failures (Keskinidis, [RISKS-21.48](#))**

Chris Kantarjiev <cak@putzl.com>  
*Mon, 18 Jun 2001 13:20:36 -0700*

> One thing is for sure, this is soon to be race against  
technology and not  
> who was the better driver on the day and as if it wasn't  
already a 2-man  
> race anyway (McLaren and Ferrari).

It's been a technology race for some time. The recent ruling to  
allow  
traction control and launch control are unfortunate but deemed  
necessary  
because some companies were pretty clearly already using them,  
despite  
efforts to police them. This is an attempt to level the playing  
field.

I find it somehow ironically satisfying that it's backfiring on  
a few of  
the players who seemed most likely to benefit from it!

> Cars can only go so fast around any track,

And how fast would that be? Tire technology (there's that word  
again) is  
constantly improving. Do you remember the active suspensions of  
8 or so  
years ago, where the in-car from Mansell's car, so equipped, was  
rock  
solid through the corners, while everyone else was skittering  
about? Did  
you miss the recent episode where CART halted a race because the  
cars  
were travelling around the Texas racetrack fast enough that  
drivers were  
starting to black out?

The teams seem to be doing live testing, all right. I can't find  
the URL  
at the moment, but Coulthard (who arguably lost the race at  
Monaco when  
his launch control failed on the formation lap, so he had to  
start from  
the back) was quoted as being pleased that the organizers had

allowed

them to do many practice starts ... and they'd all been flawless.

I think the teams just don't know what and how to test, yet. Or, at least, McLaren don't.

---

## ✶ The magic, fast-food, wand (Re: McDonald's, [RISKS-21.43](#), 21.46)

Rob Slade <rslade@sprint.ca>

*Fri, 15 Jun 2001 07:29:27 -0800*

Both RISKS readers and Bruce Schneier's June 15th CRYPTO-GRAM have noted some potential problems with McDonald's proposal to use the FreedomPay and FasTrak payment systems.

As I read

[www.usatoday.com/life/cyber/tech/2001-05-29-mcdonalds-e-payments.htm](http://www.usatoday.com/life/cyber/tech/2001-05-29-mcdonalds-e-payments.htm)

I was mentally ticking off all the reasons I couldn't see much advantage to using this type of procedure in a fast food restaurant. I don't use drive-through venues all that much, so I'm not used to paying for my food with my keys. (And consider the drive-thru: at the second window, are you really going to turn off the engine, take out your keys, swipe the wand, put the keys back in the ignition, and stall out repeatedly while the guy in the monster truck behind you leans on his horn?) I've already got enough keys that my key case is awkward. Anything smaller than a pocket knife is going

to be hard to find in my "change" pocket. The possibility of losing a tiny item that is keyed to my credit card, and possibly not finding out until the next statement comes is disturbing. And, yes, the assertion that "participants can `load' their FreedomPay account via the Internet or over the phone" would seem to allow the possibility of being defrauded even if you don't participate in the trial.

But as I was considering the actual transaction in the store, I started to wonder about the stated reasons *\*for\** using the system. It isn't going to make the purchase any faster for the customer. Consider the usual situation at the moment. You order. The cashier starts to put together your meal, but if you want anything more than a standard dark, carbonated beverage, there generally comes a point at which the hunting-and-gathering process is stymied: there aren't enough "fries," or you've ordered a salad "wrap" (you health food freak, you), or you don't want *\*that\** much mayonnaise (I'm sorry, "chicken sauce") and so something needs to be made before your order can complete. At this point the cashier returns to the till (leaving your "shake" under the hot lamp and your nuggets beside the "soft serve" freezer), takes your money and gives you your change. Then you wait some more, and finally get your food units.

So, does the possession of a wand save you, the customer, any time? Generally speaking, the answer will be "no." Does the fast food chain gain many sales because you have a McDonald's wand, and not one for Burger King?

The respective chains will have their own religious marketing beliefs in that regard, but, again, the answer is much more likely to be, "no." The three factors in the success of a restaurant have always been, in order of priority, location, location, and location. McDonald's and its ilk aren't keen on participating in "food court" situations where you have a choice, and where the possession of a wand might have tipped the scales in their favour. So why are they keen on the idea?

The most likely reason would seem to involve that cashier. Even at minimum wage, the cost of processing an order and dealing with cash has to run about thirty to seventy cents per order in wages, plus additional costs. Once the capital costs of a wand system are covered, the cost of the billing part of the order can be reduced to an almost arbitrarily low figure. And, was it not McDonald's who recently did a trial with a terminal where patrons could compose their orders, and then pick them up at the counter? With both systems in place, the joint moves one step closer to becoming a giant vending machine (albeit with much less choice than an Automat), where you punch buttons, wave your wand, and wait for the bag to thump into the slot. (And wait. And wait ...) Eliminate those pesky employees, and you eliminate costs.

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>

---

## ✶ QWE2001: Call for Papers and Presentations (PGN-ed)

<sr@linux20292.dn.net>

Sat, 16 Jun 2001 12:16:04 -0700

5th ANNUAL INTERNATIONAL INTERNET & SOFTWARE QUALITY WEEK EUROPE  
2001

12-16 November 2001

Brussels, Belgium EU

CALL FOR PAPERS AND PRESENTATIONS

<<http://www.qualityweek.com/QWE2001/call.html>>

SR/INSTITUTE, 901 MINNESOTA, SAN FRANCISCO, CA 94107 USA

Phone: [+1] (415) 550-3020 FAX: [+1] (415) 550-3030

WebSite: <<http://www.soft.com/QualWeek/QWE2001>>

Email: qw@soft.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 21: Issue 50**

**Thursday 12 July 2001**

## Contents

- [Microsoft bug causing serious nuclear risk?](#)  
[Dudi Feuer](#)  
[Michael D. Levi](#)  
[John Lowry](#)
- [Fiji has to relive Y2K?](#)  
[James Paul](#)
- [Intruder crashes United Arab Emirates' only ISP](#)  
[Dave Stringer-Calvert](#)
- [\\$480,000,000 for sending 9 parcels](#)  
[Mark Brader](#)
- [Uncleared disk space and MSVC](#)  
[David Winfrey](#)
- [Berlin Bank shows sensitive information](#)  
[Debora Weber-Wulff](#)
- [Power outage means wheel chairs on the go](#)  
[Ray Todd Stevens](#)
- [Electoral fraud](#)  
[Tony Finch](#)
- [Risks in inept election fraud](#)  
[knhaw](#)

- [Yet another e-mail filter effect](#)  
[Jurjen N.E. Bos](#)
  - [Re: Billboard error message](#)  
[Ben Morphett](#)  
[Markus Peuhkuri](#)
  - [REVIEW: "Fundamentals of Network Security", John E. Canavan](#)  
[Rob Slade](#)
  - [16th Annual Software Engineering Symposium 2001](#)  
[Carol Biesecker](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

## ⚡ Microsoft bug causing serious nuclear risk?

Dudi Feuer <dudi@yucs.org>  
*Wed, 11 Jul 2001 12:14:26 -0400 (EDT)*

According to an article in *\*The Washington Post\**, the US lent Russia programs with a bug that loses track of nuclear materials over a period of time. The software has been in use for 10 years, and the latest patch did not create a fix for the issue. Apparently, the Russians initially thought the bug was a trojan horse authored by the US. Then, after applying several patches, they realized it was an inherent flaw in the program, and most likely exists in the Los Alamos version as well.

[Source: *\*The Washington Post\**, 11 Jul 2001, A19  
<http://www.washingtonpost.com/wp-dyn/opinion/A44053-2001Jul10.html>]

---

## **Microsoft bug causing serious nuclear risk?**

Levi\_M <Levi\_M@bls.gov>

Thu, 12 Jul 2001 10:43:21 -0400

[...] The article goes on to say that the U.S. was warned of the security risks but has made no public comment on the matter. The article also points out that the U.S. no longer maintains (and indeed has destroyed) backup paper copies of their inventory: "To reconstruct a reliably accurate accounting record, the Energy Department may need to inspect all of America's nuclear materials -- a huge task that could cost more than \$1 billion and still might not detect the diversion of some material, should it have occurred."

Among other obvious risks is -- always look gift horses in the mouth.

Michael D. Levi, Project Manager, Data Dissemination Systems  
U.S. Bureau of Labor Statistics (202) 691-5100

---

## **Microsoft bug causing serious nuclear risk?**

"John Lowry" <jlowry@bbn.com>

Thu, 12 Jul 2001 10:42:50 -0400

[Re: <http://www.washingtonpost.com/wp-dyn/opinion/A44053-2001Jul10.html>]

LANL supplies MS software to Russia for nuclear material

accounting that  
develops data "black-holes" over time.

DoE has apparently abandoned paper trails and so, aside from the  
ability to  
misappropriate nuclear material that has "disappeared" from the  
database,  
there is going to be substantial cost incurred to inventory  
everything -  
even assuming nothing is missing.

What ever happened to assurance testing for critical software ?

Where else is this software being used, and for what?

John

---

## **✶ Fiji has to relive Y2K?**

"James Paul" <James.Paul@mail.house.gov>

*Thu, 12 Jul 2001 17:26:55 -0400*

A programming error resulted in the deletion of all Fiji  
Government accounts  
for the year 2000 and the postponement of official audits.  
There is  
reportedly some speculation about a cover-up of "mismanagement  
or abuse of  
taxpayer funds", although the simple solution of a screw-up  
seems likely.  
The information system dates from the mid-1970s. Presumably the  
various 52  
government ministries and departments can retransmit the  
relevant data.  
[Source: Computer error deletes all Fiji Government accounts,  
Agence  
France-Presse, 11 Jul 2001, from the \*Fiji Times\*, 12 Jul 2001]

## **✶ Intruder crashes United Arab Emirates' only ISP**

Dave Stringer-Calvert <dave\_sc@csl.sri.com>

*Tue, 03 Jul 2001 18:33:20 -0700*

A computer whizzkid has been fined £2,000 (\$2,600) for hacking into the United Arab Emirates' only Internet provider and causing the whole country's system to crash. Lee Ashurst, 22, originally from Oldham in Greater Manchester, was convicted of misusing equipment, services or facilities provided by Emirates Telecommunications Corp Etisalat. Ashurst, who works for a construction company in the Gulf, is now facing a compensation claim of more than £500,000 (\$650,000) from Etisalat after the Dubai Court of First Instance transferred his case to the civil courts. He was working as a computer engineer at a Dubai construction firm in May last year (00) when he began hacking into Etisalat's systems. According to the Gulf News newspaper, the court was told the entire United Arab Emirates internet system crashed on several occasions over a month.

[http://63.108.181.201/2001/07/03/eng-wenn/eng-wenn\\_001056\\_76\\_4245186652988.html](http://63.108.181.201/2001/07/03/eng-wenn/eng-wenn_001056_76_4245186652988.html)

---

## **✶ \$480,000,000 for sending 9 parcels**

Mark Brader <msb@vex.net>

*Thu, 12 Jul 2001 11:16:08 -0400 (EDT)*

Edward Rudzki (whose hobby shop in Edmonton, Alberta, Canada, opened in the mid-1960s) just received a bill from Canada Post for CA \$480,000,000 (roughly US\$310,000,000), for transactions supposedly having taken place from 1906 to 1928! The actual transactions were 9 parcels from a month ago, but the dates and dollar amounts were wrong. Canada Post says the problem occurred when they merged 60 databases into one. [Source: \*Toronto Star\*, 12 Jul 2001]

Mark Brader, Toronto

---

## **✶ Uncleared disk space and MSVC**

David Winfrey <dlw@patriot.net>  
*Thu, 12 Jul 2001 14:20:52 -0400 (EDT)*

I have a program called "clrspace" which clears the unused space on my hard disk. When I use it at work, I set it to fill the space with the company name and phone number.

Recently I got a new copy of the Microsoft Visual C++ compiler, version 6, introductory edition.

Today, after compiling a program of the "Hello World" level of complexity and finding that the resulting program was well over 100 kilobytes, I went to the DOS prompt and looked at the .EXE file with a hex editor

to try to  
find out why it was so big.

I was surprised to find "Property of Acme Widgets, 301-555-1212"  
in the .EXE  
file from 0x6000 to 0x14FFF. The compiler had obviously just  
grabbed a big  
chunk of disk space and stuffed it into the file, without  
bothering to clear  
it first.

If that particular chunk of disk had been used for something  
confidential,  
and if this were the production version of the compiler that  
allows  
redistribution of executables (the intro version doesn't,  
although this  
restriction is somehow omitted from the outside of the package),  
then 60  
kilobytes of company plans, source code, spreadsheets, customer  
lists, or  
whatever could have been burned onto CD and shipped to customers  
around the  
world.

Anyone compiling programs with MSVC may want to examine the  
output closely  
for data that shouldn't be there.

---

## **🔥 Berlin Bank shows sensitive information**

Debora Weber-Wulff <weberwu@fhtw-berlin.de>

*Mon, 09 Jul 2001 12:38:37 +0200*

On 2 Jul 2001, a reporter for a local newspaper wanted to check  
his on-line  
account with the Berliner Sparkasse. Imagine his surprise to  
find lots of  
interesting data about an account and loans - except that they

were not his.

About 50 persons could not access their own accounts, they were presented with data from other people. The bank assures us, that no funds could be transferred, it was "just" possible to see how much money was in the accounts and to see the last transactions.

They immediately removed the on-line banking from the net. The official problem source, according to a spokesperson from the bank, was "strain" (Ueberlastung) on the systems. The company DefCom Security worked feverishly to get it back on line by Tuesday, but forgot that they had fooled with the certificates. Users were presented with a screen warning them that the certificate was issued by a company that was classified as not trustworthy.... Maybe it's time to change banks?

If you read German, you can find more information at

<http://www2.tagesspiegel.de/archiv/2001/07/03/ak-in-6611353.html>

<http://www2.tagesspiegel.de/archiv/2001/07/03/ak-be-447917.html>

Prof. Dr. Debora Weber-Wulff

FHTW Berlin, FB 4, Internationale Medieninformatik

Treskowallee 8, 10313 Berlin

Tel: +49-30-5019-2320

Fax: +49-30-5019-2300

weberwu@fhtw-berlin.de

[http://www.f4.fhtw-berlin.de/people/](http://www.f4.fhtw-berlin.de/people/weberwu/)

[weberwu/](http://www.f4.fhtw-berlin.de/people/weberwu/)

---

## **⚡ Power outage means wheel chairs on the go**

"Ray Todd Stevens" <raytodd@kiva.net>

*Thu, 12 Jul 2001 14:27:54 -0500*

I witnessed an interesting failure mode during a recent shopping trip. This store had some of the motorized-chair shopping-cart setups for customers who need them. They are all lined up against one wall facing out and plugged into the wall charging. All was well until the power failed.

When the power failed, all of these units took off and most ran into things before the staff could stop them, trailing their cords behind them. I asked about this. It seems that there are several what appear to be glaring design flaws in these units.

1. The stopped position on the handle is not the default position. Instead, the control is all the way down for forward, all the way up for reverse and half way in between for neither. Meaning that the nature position is forward.
2. There is also a foot brake, but it must be pushed to stop.
3. Of course there is a power switch. But it must be turned on to charge the unit.

What you do to charge is plug the unit in, and then turn on the power. The fact it is receiving outside power switches it to charge mode and the unit will not go anywhere.

Now here comes the power failure. All of these units (about 7) are turned on, brake off, and in forward. They seem to assume that no electricity means that they are now to take off and do so driverless.

Interesting failure mode, and in this time of more and more backup power for computers, one we should remember.

Ray Todd Stevens, Senior Consultant, Stevens Services (812) 279-9394

R.R. # 14 Box 1400 Apt 21, Bedford, IN 47421 Raytodd@kiva.net

---

## ✶ Electoral fraud

Tony Finch <dot@dotat.at>

*Thu, 12 Jul 2001 02:00:15 +0100*

Following the question "Does the UK have significantly less electoral fraud than countries which use untraceable ballot papers?" I wrote this, which (although it is a bit late to be a followup to the discussion around last year's USA presidential election) might be interesting.

One of the interesting things about the recent general election is that fraud has been much easier to perpetrate than usual, but without any kind of extra auditing.

The reason that fraud has been worse is because they have increased the availability of postal votes. Now, this doesn't inherently imply fraud, so I will tell you a tale to explain why I think this is the case.

The usual arrangement for an election in the UK is as follows: You have (at some point in the past) put yourself on the electoral register by

filling in a form that says "I live here and this is my name and I am entitled to vote", and this means that (amongst the dead tree spam) you receive a piece of card through the letterbox shortly before an election which explains where you have to go to vote and what your voter number is. Now, you might expect (being good RISKS readers and all that) that this piece of paper is a physical token that entitles you to vote (and the process of registering entails some kind of behind-the-scenes checking that this is true), but no. You do not have to take the card to the polling station: you merely have to turn up and state your name, the only checking being that you have already put your name on the list.

Now, regardless of how bad that is, it gets worse. In the past, postal votes were quite hard to get, i.e. (unlike usual votes) some checking happened. This was because most postal voters were disabled or expatriates or had some other unusual difficulty that prevented them from getting to the polling station on the day, so there were few enough of them that checking their applications was feasible. The unique thing about this year is that large numbers of farmers and other members of the rural community have not been able to leave their homes because of the travel restrictions caused by the Foot And Mouth epidemic.

The procedure for postal votes this year has been: (1) find out the phone number you need to call to get a postal vote; (2) say to the person on the other end of the line how many votes you need; (3)

receive the forms through the post; (4) fill them in; (5) sit back and enjoy an extra-large swing in your constituency. If you think that you might not have enough votes, feel free to call back again later and ask for more. [I know someone who tried this out to see if it worked, and it did, but I don't think he actually used the extra votes.]

The general election this year has been characterised by an unusually large degree of apathy (59% turn-out, compared to usually 75% or so) but the aggregate result has been just as conclusive as the 1997 result (71% turnout): a landslide victory for the Labour party. The per-constituency change in opinion has made almost no difference to the membership of the House of Commons. This means that there has been absolutely no worry about electoral fraud, since it couldn't have made a significant difference to the overall result.

The interesting thing is that the small turnout is likely to have a greater long-term effect than any murmurs of procedural irregularities: the proportional-representation faction have made great mileage from saying that people are apathetic because they have no control over politics, and they have no control because they live in a safe constituency, so their third-party Lib-Dem vote counts for nothing. They have made further headway because of the Gothenburg summit riots which were perceived to be a complaint against the unrepresentative ivory towers of the EU politicians.

So, even though the Brits don't want to look like pillocks for criticising the Americans for their banana republic election, we changed none of the procedures, had another shambolic election, and breathed a sigh of relief because it was a cock-up that didn't matter. It remains to be seen whether those in favour of electoral reform will be able to maintain their momentum and get a better system working before the next time.

---

## ✶ Risks in inept election fraud

<knhaw@rockwellcollins.com>

*Wed, 27 Jun 2001 09:44:16 -0700*

Several news outlets are reporting on the recent "No Contest" plea on June 14th by Christine Gunhus, wife of former U.S. Senator Rod Gram (Republican, Minnesota) on criminal violations of Minnesota election code. Here is the posting from Cluebot.com, which reads suspiciously like a RISKS posting ;)

The wife of a U.S. senator who unsuccessfully ran for re-election in 2000 plead "no contest" on Thursday to charges of using a pseudonym to send email messages that disparaged her husband's Democratic rival.

Minnesota prosecutors charged Christine Gunhus, who married former Republican senator Rod Grams after working on his campaign, with violating state criminal laws. Grams' rival, Democratic-Farmer-Labor candidate Mike

Ciresi, had filed a complaint under the Minnesota Fair Campaign Practices Act.

The risks of using technology you don't completely understand and that could leak your identity are worth noting:

\* Gunhus is accused of using a Hotmail account (Katie Stevens -- kylomb@hotmail.com) to send the disparaging email messages, which talked about how Ciresi had represented corporate polluters and anti-union companies. But Hotmail includes an X-Originating-IP: header that shows the IP address of the sender -- a problem if you're typing it from the opposing campaign's computer!

\* Prosecutors say they traced the IP address back to an AT&T WorldNet user who repeatedly used the "Katie Stevens" Hotmail account by connecting from Gunhus' home number. (Guess they keep Caller ID logs.) Apparently the person using the "Katie Stevens" pseudonym was smart at first, sending the mail from a Kinko's store, but then got sloppy.

\* The email attacks included Microsoft Word attachments, which a Ciresi aide investigated. The aide found that Word listed the document authors as Grams staffers including -- you guessed it -- Christine Gunhus.

\* Democratic researchers reported that they found Globally Unique Identifiers (GUIDs) in the Word documents. The GUID includes the Ethernet MAC address. Prosecutors last August obtained a search warrant to seize Gunhus' computer, from which they could extract the MAC address if the

Ethernet card was still the same.

\* Let's not forget the political risk. In an article in the Minneapolis Star-Tribune on the pseudonymous mail campaign last year, the Grams campaign offered a remarkably narrow denial. A spokesman hedged: "We didn't put this together and send it out of the Grams campaign office," leaving open the question of whether it was sent by a campaign worker from another location.

\* And what about the legal risk to free speech? The Minnesota Civil Liberties Union reasonably argues that a criminal law that bans sending pseudonymous messages is unconstitutional. A Supreme Court decision, *McIntyre v. Ohio Elections Commission* ([http://www.epic.org/free\\_speech/mcintyre.html](http://www.epic.org/free_speech/mcintyre.html)), says that a prohibition on the distribution of anonymous campaign literature violates the First Amendment. The state law seems to be ecumenical in its application: A Republican has used it to attack the Sierra Club ([http://www.fcregister.com/ziegler11\\_6\\_00.htm](http://www.fcregister.com/ziegler11_6_00.htm)).

Epilogue: Grams managed to derail his Democratic rival's primary bid, and Ciresi did not win his party's nomination. Even though Grams lost the general election in the fall, that hasn't halted his political ambitions. The Washington Times reported on April 13 that Grams is reportedly considering a challenge in 2002 to U.S. Senator Paul Wellstone, a liberal Democrat. "

Cluebot story (with links):

<http://www.cluebot.com/article.pl?sid=01/06/15/0135212&>

mode=nocomment

Minnesota Public Radio story on original affidavit:

[http://news.mpr.org/features/200009/08\\_radila\\_grams/index.shtml](http://news.mpr.org/features/200009/08_radila_grams/index.shtml)

---

## **✶ Yet another e-mail filter effect**

<j.bos@interpay.nl>

*Wed, 27 Jun 2001 09:47:41 +0200*

The IACR (International organisation of Cryptology Research) has someone on its Board of Directors named Don Beaver. The direct result of this is that the recent IACR newsletter (a 34K document full of relevant news on the cryptologic community) was rejected by our company firewall, because his name was in there too many times. It also contained other "dirty" words, such as LaTeX, hardcore, and so on.

Our IT department told me that the message would *\*not\** have been rejected if it was split in two, since the number of dirty words would have been halved.

X-|

Sigh. I thought cryptology was to prevent us from this kind of misery.

Jurjen N.E. Bos, Risk Management / Information Security Services  
Interpay Nederland BV, Postbus 30500, 3503 AH Utrecht tel. +31  
30 283 6815

---

**✉ Re: Billboard error message ([RISKS-21.45,46,48](#))**

Ben Morphett <morphett@lucent.com>

*Fri, 08 Jun 2001 10:40:25 +1000*

> I was driving on I-405 northbound in southern Los Angeles  
County when I saw  
> a bitmapped billboard on the east side of the road that was  
displaying a  
> Windows error message.

Recently I was on a carnival ride called "The Drop Zone" with my  
nephews  
when I saw a similar Windows error message.

The Drop Zone is rather fun. They strap you in the ride, you  
are lifted  
to the top of a tower, about 100m from the ground. There are  
computer  
screens at the top which give you a narrative about how some  
spacecraft  
is going down and the whole crew are going to have to bail out,  
and then  
they drop you. You experience free fall for a few seconds. The  
kids  
scream. You land safely.

The second time we did the ride, we got to the top and Windows  
had  
crashed. This time it was my turn to scream. "I *\*really\** hope  
my life  
is not depending on Windows right now! It's crashed!"

Ben Morphett, Bell Labs Research & Development

---

**✉ Re: Billboard error messages ([RISKS-21.45,46,48](#))**

Markus Peuhkuri <puhuri@tct.hut.fi>

*Tue, 19 Jun 2001 11:46:24 +0300 (EET DST)*

> signs that was declaring in foot-high letters "BATTERIES NEED RECHARGING".

That may be all that stupid if the system has no other way indicating problems (some better formulation like "Malfunction: .." could help).

But, if it has some other means to inform operator, then it is stupid.

> The general risk, of course, is in piping STDERR to STDOUT.

Web  
> sites that send complex error dumps to visitors' browsers are doing

There is a more risk than just user just being stumped by obscure messages. In many cases I've seen the error message has revealed quite much of internal workings of web service. I remember even seeing something like

```
db_connect(user=db, passwd=pass): failed no connection
```

The security risks are obvious.

Markus Peuhkuri ! <http://www.iki.fi/puhuri/>

---

## **🔥 REVIEW: "Fundamentals of Network Security", John E. Canavan**

Rob Slade <rslade@sprint.ca>  
*Mon, 25 Jun 2001 12:18:24 -0800*

BKFNNTSC.RVW 20010512

"Fundamentals of Network Security", John E. Canavan, 2001,  
1-58053-176-8, U\$69.00

%A John E. Canavan canavan@well.com jcnv@chevron.com  
%C 685 Canton St., Norwood, MA 02062  
%D 2001  
%G 1-58053-176-8  
%I Artech House/Horizon  
%O U\$69.00 617-769-9750 fax: 617-769-6334 artech@artech-house.  
com  
%P 319 p.  
%T "Fundamentals of Network Security"

This commonplace guide to security can provide the newcomer with some basic information. However, it also contains some rather large gaps, and not a little misinformation.

Chapter one outlines the usual reasons why we need security, and it also provides some basic security terms and concepts. Most of the material is reasonable, but some is not quite standard. A number of different threats are outlined in chapter two. However, errors are rife in this material, although most are fairly minor. Of the fourteen mailing lists it is suggested readers might find useful, at least three have been dead for over a year; at least two of those for more than three. The overview of cryptology, in chapter three, is at a very high level, with limited discussion of key management, and almost none dealing with strength and key length. Chapter four starts out very badly, by stating that Kerberos uses both symmetric and asymmetric cryptography. (It doesn't: despite proposals for public key extensions, Kerberos itself uses a very elegant system of purely private key encryption to avoid sending passwords and keys in clear text at any time. Such a basic misunderstanding taints

everything else in the chapter.) World Wide Web encryption is supposed to be the topic of chapter five. However, after a very terse outline of SSL (Secure Sockets Layer) and SHTTP (Secure HyperText Transfer Protocol), and a tiny bit of the missing discussion of key length, we get pages of screen shots of browser certificates, which are almost meaningless without the background review. There is also a tiny overview of Authenticode, with no mention of its flaws. Chapter six presents something of a grab bag of email related topics, mentioning encryption systems, spam, identity problems, privacy of employee email, and even auto-responders. With the addition of more screen shots a number of pages are taken up with little information imparted.

Most of chapter seven concentrates on access control and passwords. The material is reasonable, if not deep, but could be better organized. So too with the suggested policies for network management in chapter eight, although the author does seem to think that one set of recommendations can fit all LANs. Chapter nine's look at network media does not really deal with security at all, unless you count the somewhat problematic opinions regarding the relative difficulty of tapping. There really isn't much discussion of routers and SNMP (Simple Network Management Protocol) in chapter ten: it concentrates on a few proprietary products.

Chapter eleven mentions a number of VPN (Virtual Private Network) related protocols, but gives neither details for assessment nor conceptual

discussions for determining relative usage. There is a decent overview of basic firewall terms, with some areas of confusion, in chapter twelve. Chapter thirteen has a basic outline of biometric concerns, but no details of the technologies. The review of security policy development in chapter fourteen is pedestrian. Chapter fifteen, entitled "Auditing, Monitoring, and Intrusion Detection," is oddly confused since the author makes no distinction between outside audits, and the ongoing auditing of materials that result from regular monitoring. There is unimaginative advice on disaster recovery in chapter sixteen. "Cookies, Cache, and AutoComplete" is a strange add-on: yes, there are security risks associated with these functions, but they are hardly fundamental to network security.

In the introduction, while stating that this book is intended for beginners to computer security, the author disclaims the title of computer security expert, and, in fact, asserts that many who do profess ace status may not have as much right as they maintain. I can greatly sympathize with this sentiment. However, simply by writing a book, Canavan implicitly professes some mastery of the subject, and the mere abdication of the rank does not relieve him of the responsibility for his mistakes. There are a number of other texts with better coverage, greater readability, superior accuracy, and less wasted space.

copyright Robert M. Slade, 2001    BKFNTSC.RVW    20010512  
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/>

---

## **16th Annual Software Engineering Symposium 2001**

Carol Biesecker <cb@sei.cmu.edu>

*Thu, 12 Jul 2001 14:07:23 +0000 (UTC)*

SEI 16th Annual Software Engineering Symposium 2001

Theme: Acquiring the Strategic Edge

October 15 - 18, 2001

Grand Hyatt at Washington Center

Washington, D.C.

<http://www.sei.cmu.edu/symposium/>

Contact: Symposium 2001 Conference Coordinator

Phone: 412 / 268-3007

FAX: 412 / 268-5556

E-mail: [symposium@sei.cmu.edu](mailto:symposium@sei.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 21: Issue 51**

**Monday 16 July 2001**

## Contents

- [CD-eating fungus amongus](#)  
[Gary Stock](#)
- [The computer is taking over the train](#)  
[Hanan Cohen](#)
- [Trains Ain't Planes, it's plain to see](#)  
[Daniel P Dern](#)
- [Eli Lilly e-mail snafu reveals identities of Prozac users](#)  
[Jeremy Epstein](#)  
[Allan Noordvyk](#)
- [Brownouts take out computers in Livermore](#)  
[Fred Cohen](#)
- [Phoenix BIOS phones home?](#)  
[Merlyn Kline](#)
- [Hacked caller ID?](#)  
[Alexandre Pechtchanski](#)
- [Anatomy of an Internet scam](#)  
[NewsScan](#)
- [Who watches the watchdog?](#)  
[Gary Barnes](#)
- [Autoresponder goes haywire](#)

[Joshua M Bieber](#)

● [Auto-banner ads](#)

[Mark Richards](#)

● [Microsoft pulls controversial Smart-Tag feature](#)

[NewsScan](#)

● [Yearly siren test ...](#)

[Marco Frissen](#)

● [4 to 6 \\*million\\* votes uncounted in 2000 election](#)

[PGN](#)

● [US Voting Systems Standards - available for public comment](#)

[Thom Wysong](#)

● [Re: Electoral fraud](#)

[David Hedley](#)

[Lindsay Marshall](#)

● [Re: WashingtonPost.com real estate database](#)

[Tramm Hudson](#)

● [Re: Uncleared disk space and MSVC](#)

[John Sullivan](#)

[Peter da Silva](#)

● [Re: The risks of clueless marketing](#)

[Toby Riddell](#)

● [10th USENIX Security Symposium](#)

[Tiffany Peoples](#)

● [Info on RISKS \(comp.risks\)](#)

---

## ✶ CD-eating fungus amongus

Gary Stock <gstock@nexcerpt.com>

Tue, 19 Jun 2001 13:22:22 -0400

>From Electronic Telegraph:

<http://www.telegraph.co.uk/et>

?ac=004299402432522&rtmo=k7bZ7bYp&atmo=rrrrrrrrq&pg=/  
et/01/6/18/wfung18.html

Scientist finds fungus that eats through compact discs

By Robert Uhlig, Technology Correspondent

FIRST there was the computer virus. Now scientists have found a fungus that eats compact discs.

Victor Cardenes, of Spain's leading scientific research body, stumbled across the microscopic creature two years ago, while visiting Belize.

Friends complained that in the hot and sticky Central American climate, a CD had stopped working and had developed an odd discoloration that left parts of it virtually transparent.

Dr Cardenes and colleagues at the Superior Council for Scientific Research in Madrid discovered a fungus was steadily eating through the supposedly indestructible disc. The fungus had burrowed into the CD from the outer edge, then devoured the thin aluminium layer and some of the data-storing polycarbonate resin.

Dr Cardenes said: "It completely destroys the aluminium. It leaves nothing behind." Biologists at the council had never seen this fungus, but concluded that it belonged to a common genus called geotrichum.

Philips, the Dutch electronics company that invented the compact disc, said it believed the Belize case was probably a freak incident caused by extreme weather conditions.

Gary Stock UnBlinking [gstock@unblinking.com](mailto:gstock@unblinking.com) <http://unblinking.com/>

## ✶ The computer is taking over the train

Hanan Cohen <hanan\_cohen@yahoo.com>

*Thu, 12 Jul 2001 08:50:58 +0200*

Overhead on the MUNI this morning: "Hang on, please. The computer is taking over the train." A feeling of dread rippled through the train.

"Finally," we all thought, "the war with the machines is beginning."

<http://www.kottke.org/notes/0107.html#010711>

Hanan Cohen - <http://www.info.org.il>

---

## ✶ Trains Ain't Planes, it's plain to see

Daniel P Dern <ddern@world.std.com>

*Wed, 20 Jun 2001 10:19:12 -0400 (EDT)*

Usually, I do my work-related travel between Boston and New York by plane, but I've been meaning to try train again, especially Amtrak's allegedly-faster Accela.

So I call the company travel office to make reservations. (I already know which trains -- whatever the rail equivalent of "flights" is -- I want.) An e-mail confirmation shows up a few minutes later, with a URL pointing to an itinerary.

The itinerary showed the correct train numbers and arrival times. No departure times.

And had me going between (something like, IIRC) Aptco Test, Texas and someplace in Arkansas.

I called the travel group back; they called Amtrak. My reservation's correct, but when the AmTrak system passed info to the next system, it tried to parse City Codes as Airport Codes.

More obvious than the "metric vs. English" glitch, but still shows that just because two programs can talk to each other doesn't mean they've agreed on what they're saying... Fortunately, if I get on a southbound train from Boston (traveling at n miles an hour accompanied by a parrot with a balloon tied to one foot) it'll be hard to miss arriving in New York.

Daniel Dern, Executive Editor, Byte.com <ddern@world.std.com>

---

## **✶ Eli Lilly e-mail snafu reveals identities of Prozac users**

"Jeremy Epstein" <jepstein@webmethods.com>

*Thu, 5 Jul 2001 18:31:50 -0400*

Eli Lilly sent an announcement that it was discontinuing a mailing list, using CC instead of BCC. Some of the more than 600 recipients were unhappy about having their e-mail addresses and Prozac use disclosed, because the purpose of the list was to send out reminders to fill

prescriptions for the anti-depressant drug. According to a \*ComputerWorld\* article, "Eli Lilly is preparing a code audit review and 'working on a program that would block all outbound e-mails with more than one address.'" The American Civil Liberties Union (ACLU) has asked the Federal Trade Commission (FTC) to investigate.

A little bit of anonymity is a good thing, even if it's not totally anonymous (e.g., a Hotmail account).

---

## ✶ Eli Lilly e-mail snafu reveals identities of Prozac users

Allan Noordvyk <anoordvyk@alitech.com>

*Thu, 5 Jul 2001 12:56:29 -0700*

This kind of error is made frequently by new users of e-mail software, but it is interesting (but perhaps not surprising) to see that corporations running large mailing lists occasionally making the same error. In either case, it's usually merely an annoyance, or a strategic embarrassment (i.e., effectively giving away your customer list to your competitors). However, in this case the desire of the patients to keep their medical condition private adds another more serious layer to the risk.

Allan Noordvyk

---

## **⚡ Brownouts taking out computers in Livermore**

Fred Cohen <fc@all.net>

*Thu, 12 Jul 2001 16:27:52 -0700 (PDT)*

On 11 Jul 2001, the power levels in Livermore, CA dropped to voltages so low that air conditioners and computers could no longer operate. Computers and air conditioning units went off and on moment by moment -- some lighting systems ended up burnt out, and those without UPSs on their computers had significant data corruption. It is especially noteworthy that this area was NOT on the areas scheduled for blackouts.

It turned out to be a set of changes they were making in the infrastructure -- half of our house became out of power, the other half still worked. We went to motor generator for the down half till we determined what was up, then switched over to a cross feed from the rest of the house. When power came back we switched back - thank you UPSs and motor generators...

Fred Cohen at Sandia National Laboratories at tel:925-294-2087  
fax:925-294-1225

Fred Cohen & Associates: <http://all.net> - fc@all.net - tel/  
fax:925-454-0171

Fred Cohen - Practitioner in Residence - The University of New Haven

---

## **⚡ Phoenix BIOS phones home?**

"Merlyn Kline" <merlyn@zynet.net>

Wed, 20 Jun 2001 10:04:48 +0100

>From slashdot: <http://slashdot.org/yro/01/06/19/2039216.shtml>

Myrv writes: "There is an interesting thread over at DSL Reports discussing Phoenix Technologies new BIOS. This BIOS contains the PhoenixNet Internet Launch System. ILS resides safely within ROM and is activated the first time a user launches a PhoenixNet-enabled PC with a Windows 98 Operating System. When the PhoenixNet ILS detects an Internet connection, it makes contact with the PhoenixNet server and delivers user-selectable services. These services are delivered to the user as hotlinks on the desktop and in the web browser or, as applications that PhoenixNet automatically packages, downloads and installs. It's 3 a.m., do you know who your motherboard's talking to????"

Merlyn Kline = merlyn@zynet.net

---

## ⚡ Hacked caller ID?

Alexandre Pechtchanski <pechtca@rockefeller.edu>

Fri, 13 Jul 2001 15:53:49 -0400

I've recently discovered an incoming number in my caller ID list that looks suspiciously as a hack. The number is listed as 212-555-1212, which is a long-distance directory assistance for New York, NY and, AFAIK, cannot be an originating number. I called Verizon Communications, which

serves both my  
home code 201 and New York's 212, and their service  
representative confirmed  
that call could not have originated from this number, but  
refused to  
speculate on why I would see it on my caller ID. I wonder how  
long will it  
take for exploits of such hole in telecommunication  
infrastructure to  
invalidate law enforcement evidence as in, say, [RISKS-21.50](#)  
article by  
<knhaw@rockwellcollins.com> on Risks in inept election fraud,  
which mentions  
that

> \* Prosecutors say they traced the IP address back to an AT&T  
>WorldNet user who repeatedly used the "Katie Stevens" Hotmail  
>account by connecting from Gunhus' home number. (Guess they  
keep  
>Caller ID logs.)

Alexandre Pechtchanski, Systems Manager, RUH, NY

---

## **⚡ Anatomy of an Internet scam**

"NewsScan" <newsscan@newsscan.com>

*Tue, 03 Jul 2001 09:54:11 -0700*

Federal investigators have charged 53-year-old mid-westerner  
Donald A.  
English with perpetrating an Internet-based "Ponzi" scheme that  
bilked tens  
of thousands of small investors out of \$50 million. In a Ponzi  
scheme, early  
investors are paid phony "profits" from the money taken from  
other investors  
who follow them, after hearing about the huge, fast profits.  
Since no money  
is really being earned, the pyramid eventually collapses, when

the supply of  
new investors diminishes. Many of the investors in English's  
operation,  
which was called EE-Biz Ventures, were people who are elderly or  
sick. One  
of them wrote: "I need at the least a full refund of the \$3,000  
spent if you  
do not intend to pay anyone back. Remember, I have cancer and  
am unable to  
work for the next six months." [\*The New York Times\*, 3 Jul  
2001,  
<http://partners.nytimes.com/2001/07/03/business/03PONZ.html>;  
NewsScan Daily,  
3 July 2001]

---

## Who watches the watchdog?

Gary Barnes <gkb@bofh.org.uk>  
*Fri, 22 Jun 2001 08:37:25 +0100*

Thousands of consumers' credit card details were leaked by a  
"flaw" on a  
(UK) Consumers' Association website, according to the BBC:  
[http://news.bbc.co.uk/hi/english/business/  
newsid\\_1401000/1401648.stm](http://news.bbc.co.uk/hi/english/business/newsid_1401000/1401648.stm)

The consumers affected were people who had bought tax  
calculation software  
from the Consumers' Association.

The ironic thing is that as a watchdog organisation for  
consumers, the  
Consumers' Association is responsible for administering the  
Which? Web  
Trader scheme which aims to make online shopping "easy and safe".

The Which? Web Trader Code of Practice at:

[http://whichwebtrader.which.net/webtrader/code\\_of\\_practice.html](http://whichwebtrader.which.net/webtrader/code_of_practice.html)

says of sites displaying the Which? Web Trader logo:

"You must have an effective security policy that you review regularly.

Your policy must include the following:

- you must ensure that your web site is secure so that consumers' personal information and transactions remain confidential and cannot be interfered with"

This incident will do more than most to make consumers aware of the RISKS of shopping on the Net, given the current level of security of Web traders' sites.

Gaz gkb@bofh.org.uk (Gary "Wolf" Barnes)

---

## **✶ Autoresponder goes haywire**

"Joshua M Bieber (852-5436)" <jbieber@vnet.ibm.com>

*Fri, 13 Jul 01 09:50:36 EDT*

I had a strange experience with one of the mailing lists that I have subscribed a week ago. I am sure that this was mentioned in the past, if so perhaps it is time for a reminder...

Basically what happened was that one of the subscribers to the mailing list decided to get a new e-mail address, and as a courtesy to those who still

use the old e-mail address, set up an autoresponder on the old e-mail address that sends the following message: (you know what got changed to protect who)

```
> From: guilty.olddaddy.com
> To: you.youraddy.com
> Subject: Re: current discussion topic
>
> Hello,
> My new e-mail address is guilty.newaddy.com
> Guilty Person
```

Ok, so what happened? Well, someone decided to post a message to the mailing list which promptly sent a copy to all subscribers. The autoresponder picked it up and posted the above message to the sender which happened to be the mailing list. The mailing list then sent a copy of the autoresponder's e-mail to all subscribers including the sender. The autoresponder then sent another e-mail to remind the mailing list of the new address. Ad infinitum.

I was surprised to see 15 such entries in my mailbox when I checked my e-mail before logging off that Sunday night. When I realized that this is what happened, I immediately notified via ICQ the owner of that mailing list who happened to be on-line and she was able to put a stop to it immediately. It isn't clear to me at this point whether she actually stopped it or the guilty person logged on at that time and put a stop to it. By the time it stopped, a total of 46 notifications were sent. This took up 100MB of my allotted 4000MB mailbox space at malaspina.com. So if this hadn't been

stopped in time, a lot of mailboxes would have been full.

So what went wrong? For starters:

- 1) Guilty Person forgot to change all mailing list subscription  
or  
more specifically, this particular one.
- 2) The autoresponder wasn't configured to send exactly one e-mail to  
any given user (or maximum of one per day).
- 3) The mailing list in question didn't have a mechanism that  
would  
recognize duplicate message body being sent over and over  
again  
and reject duplicate submissions.

I notified the mailing list site with a copy of the offending e-mail  
explaining what happened and asked them to do what they can to  
prevent this  
from happening again. The mailing list owner deleted the  
duplicate entries  
from the archives and Guilty Person apologized.

---

## **⚡ Auto-banner ads**

"Mark Richards" <mark.richards@massmicro.com>

*Thu, 12 Jul 2001 21:40:06 -0400*

As reported in last weeks' NTK digest (<http://www.ntk.net>), auto-generated  
banner ads (particularly when appearing in news pages) can  
generate  
significant embarrassment.

NTK illustrates it at <http://www.ntk.net/2001/07/06/dohburn.gif>  
however they are not certain as to its authenticity.

At any rate, having a banner ad titled "Burn baby, burn" (a reference to a CD ROM burner) above a story titled, "One toddler dead, another critical after house fire", certainly brings home the point.

With mindless automation, the embarrassment possibilities are infinite.

---

## **Microsoft pulls controversial Smart-Tag feature (Re: [RISKS-21.46](#))**

"NewsScan" <newsscan@newsscan.com>

*Thu, 28 Jun 2001 09:18:41 -0700*

Bowing to a wave of criticism, Microsoft says it will kill plans to include a Smart Tag feature in its forthcoming Windows XP operating system. The feature would have allowed Internet Explorer to turn any word on any Web site into a link to Microsoft's own sites and services, or to a site of Microsoft's choosing. The company continues to defend Smart Tags in principle, and plans to work toward including it in a future version of Windows or Internet Explorer, but group VP Jim Allchin said the decision was made to remove the Smart Tags because "we got way more feedback than we ever expected." Although many people view the public reaction against Smart Tags as excessive, Wall Street Journal columnist Walter Mossberg says, "...Microsoft's dominant Internet Explorer browser is like a television set, or a digital printing press, for the Web. Its function is to render -- accurately and neutrally -- all Web pages that follow standard

programming... Microsoft has a perfect right to produce and sell its own Web content with its own points of view. But it is just plain wrong for the company to use the browser to seize editorial control and to steal readers from other sites." [\*Wall Street Journal\*, 28 Jun 2001 <http://interactive.wsj.com/archive/retrieve.cgi?id=SB993679289461737795.djm> (sub req'd); NewsScan Daily, 28 June 2001]

---

## **Yearly siren test ...**

<marco.frissen@philips.com>  
*Thu, 7 Jun 2001 13:39:58 +0200*

On 6 June 2001, 12:00, 12:05 and 12:10 were targeted for the siren test in the Netherlands. The sirens are used to warn people if a catastrophe has happened (remember Enschede, fireworks factory), or war has started. In the past, when sirens were still mechanical, these tests occurred once every month (first Monday of the month). Now, everything is computerised, and 'they' have decided to test only once a year. Well, after the test this time, a lot of sirens did not work at all, or some started to late. In Limburg, a province in the south, 6 sirens refused work, due to a software glitch. In Groningen, in the North, also. Other areas were also 'silent'.

Because the new sirens have high-tone 'woops', the sound doesn't travel nearly as far as the old sirens. If one fails, there's little

chance of  
hearing another for people living close to the 'silent' siren.  
The Risk?  
Only your life...

Marco Frissen      CryptoWorks

---

## ✂ 4 to 6 \*million\* votes uncounted in 2000 election

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

*Mon, 16 Jul 2001 14:05:13 PDT*

One person, one vote? NO. And Florida was not the worst state. According to the Caltech/MIT study, Illinois, South Carolina, Idaho, Wyoming, and Georgia had even higher rates of uncounted ballots. In all, up to 2 million ballots were discarded because of faulty/aged equipment or poorly designed ballots; up to 3 million due to registration foul-ups; up to another million or so because of polling-place screwups; and an unknown number of absentee ballots discarded.

<http://www.cnn.com/2001/ALLPOLITICS/07/16/voting.problems/index.html>

And the 15 Jul 2001 issue of \*The New York Times\* had several articles documenting widespread irregularities in the counting of absentee ballots in Florida.

---

## ✂ US Voting Systems Standards - available for public comment

Thom Wysong <wysong@technodemocracy.org>

*Mon, 02 Jul 2001 22:35:36 -0400*

The US Federal Election Commission (FEC) has made available for public comment an updated version of their Voting Systems Standards (VSS). The original US VSS were published in 1990. They have gone unrevised until now. The draft for the updated "Volume 1: Voting System Performance Standards" is currently available. The draft for the updated "Volume 2: Voting System Test Standards" is scheduled to be released for public comment in late 2001.

The FEC press release is at <http://www.fec.gov/press/062801nvra.html>

An overview of the Voting Systems Standards is at <http://www.fec.gov/pages/standardsoverview.htm>

The current draft of VSS Volume 1 is at <http://fecweb1.fec.gov/pages/vss/062801vss.html>

Comments may be submitted to the FEC at [vss@fec.gov](mailto:vss@fec.gov).

---

## **✶ Re: Electoral fraud (Finch, [RISKS-21.50](#))**

David Hedley <dhedley@hebdenbridge.u-net.com>

*Fri, 13 Jul 2001 14:13:40 +0100*

While not disagreeing that fraud in UK Elections has been made easier by easing restrictions on postal votes, things are not as bad as

Tony Finch  
implies.

The procedure is as reported - I can phone and ask for as many forms as I wish. But I can't just sit and fill them all in. To obtain a postal vote, it is necessary to be on the electoral register to start with. If you are on the register, then you can fill in one form for a postal vote, and receive your postal vote. In the past, you were expected to vote in person unless there was a good reason not to do so. Now, anyone may obtain a postal vote. The voting papers are then sent to your address for you to fill in and return by post. You are blocked from voting in person. Filling in a second form (for the same voter) does not acquire an extra vote!

The system is open to fraud. To get on the electoral register is easy. All there is to do is list the people who live at an address on a particular date and who are eligible to vote. It is presumably easy to add a few names at this stage. It is also not unknown for impostors to vote, especially for dead people. It is extremely rare, however, for an impostor to vote instead of a living person.

There is now an extra potential for fraud. In the past, postal votes could only be obtained for one vote at time. Now it is possible to obtain a postal vote for life, no matter what changes of address occur.

I can also assure Tony that many Brits are happy to criticise the US "banana republic election" and don't feel pillocks for doing so.

I am happy that (a) my [postal] vote was counted, (b) I was not barred from voting because I lived in a black neighbourhood and/or may have once had a conviction, (c) the voting process and checking of electoral lists is not in the hands of a political party, (d) the judges who rule on the validity of the voting are not appointees of a political party.

And, of course, the party with the most votes won the election.

David Hedley

---

## ✶ Re: Electoral fraud (Finch, [RISKS-21.50](#))

<Lindsay.Marshall@newcastle.ac.uk>

*Fri, 13 Jul 2001 11:04:58 +0100 (BST)*

Tony Finch describes the process for getting postal vote in the UK. His description does not match my experience at all. Yes, I had to phone a number, but I was then sent an \*application\* form which I had to fill in and return. There was never any opportunity a) for saying how many votes I wanted or b) for getting more vote forms. (I should also add that there was never any opportunity for me to vote either as the post office managed to take over a week to deliver my application and so I missed the closing date for applications so I never even got to see a postal vote form)

<http://catless.ncl.ac.uk/Lindsay>

## ✶ Re: WashingtonPost.com real estate database

Tramm Hudson <hudson@swcp.com>

18 Jun 2001 23:50:14 GMT

Nick Laflamme <dplaflamme@alumni.nd.edu> wrote in comp.[risks\\_21.49](#):

> WashingtonPost.com, in association with a local real estate agency, has put  
> up a database of home sale prices and property tax appraisal values.

I had to check the price for the most famous address in the DC area,  
2600 Pennsylvania Ave NW. According to the database, it is owned by  
the Exxon Corporation, has zero bathrooms and was assessed at US \$1.3M.

My screenshot of the listing is available here:

<http://www.swcp.com/~hudson/whitehouse.html>

The risks are obvious...

hudson@swcp.com hudson@turbolabs.com <http://www.swcp.com/~hudson/>

W 505.986.60.75 KC5RNF @ N5YYF.NM.AMPR.ORG

[NOTE: This item would be interesting were the White House at 2600

instead of 1600 Pennsylvania. Indeed EXXON owns 2600. Your moderator

apologizes for letting this one slip by. PGN]

---

## **Re: Uncleared disk space and MSVC (Winfrey, [RISKS-21.50](#))**

John Sullivan <[john@kanargh.force9.co.uk](mailto:john@kanargh.force9.co.uk)>

*Fri, 13 Jul 2001 03:40:16 +0100*

> Anyone compiling programs with MSVC may want to examine the  
output closely  
> for data that shouldn't be there.

Well, it's not really MSVC's fault - it is definitely the  
operating system's  
job to make sure that no sensitive data is leaked from one  
process to  
another, in any way whatsoever. If MSVC exhibits this behaviour  
then it  
could just as easily happen to Word or any other application,  
and I bet your  
company sends out far more Office documents than finished  
executables.

You didn't mention what OS or filesystem you were running. If it  
was Windows  
95/98/ME or NT on a FAT filesystem, then it would still be a  
seriously bad  
defect, but one I wouldn't be *\*too\** surprised to see existing.  
If it was NT  
on an NTFS filesystem, then it is absolutely unforgivable  
because that's  
exactly the sort of leak it claims to prevent.

And don't forget that even if your OS doesn't leak sensitive  
information via  
disk or memory allocations, most compilers *\*deliberately\** leak  
small  
amounts of information identifying the build environment - for  
example gcc  
puts dummy symbols "gcc2\_compiled." in all object files which  
you have to be  
careful to strip out if that's important to you. Not that I  
imagine it's too  
hard to identify a compiler without such blatant clues.

## ✦ **Re: Uncleared disk space and MSVC (Winfrey, [RISKS-21.50](#))**

Peter da Silva <peter@abnm.com>

*13 Jul 2001 12:59:48 GMT*

It's not the compiler's fault, it's the operating system's fault. Application programs should never have a mechanism that lets them look at the contents of unallocated blocks.

Actually, it may not even be the operating system's fault.

I suspect your "clearspace" program overwrote some blocks the OS thought were already cleared. If they use a "block clearing daemon" to clear unallocated blocks in the background, your program could have caught them after the daemon had passed them by.

Still, I can't think of any reason for the OS to actually read cleared blocks off disk. They should hand out a freshly zeroed block of memory and write it to disk later. . . possibly it did do that, then since the compiler never modified those blocks it didn't write them back to disk since they were already clear.

A risk of using third-party utilities that modify things without informing the OS?

---

## ✦ **Re: The risks of clueless marketing (J.McCarthy [RISKS-21.46](#))**

Toby Riddell <tobyridell@yahoo.com>

Sun, 1 Jul 2001 08:10:20 -0700 (PDT)

chi-rho sounds rather like Cairo. I don't follow Microsoft all that closely but wasn't this one of their codenames?

[also noted by Craig Cottingham. PGN]

---

## 🔥 10th USENIX Security Symposium

Tiffany Peoples <tiffany@usenix.org>

Mon, 16 Jul 2001 10:14:58 -0700

10th USENIX Security Symposium  
August 13-17, 2001, Washington, D.C.

For more information and to register, visit:

<http://www.usenix.org/events/sec01>

REGISTER BY JULY 20, 2001 AND SAVE UP TO \$200!

The 2001 10th Security Symposium is sponsored by USENIX, the Advanced Computing Systems Association. [www.usenix.org](http://www.usenix.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 21: Issue 52**

**Tuesday 17 July 2001**

## Contents

- [Subject: Re: WashingtonPost.com real estate database](#)  
[PGN](#)
- [Info on RISKS \(comp.risks\)](#)

---

✶ **Re: WashingtonPost.com real estate database (Hudson, [RISKS-21.51](#))**

"Peter G. Neumann" <neumann@csl.sri.com>  
*Tue, 17 Jul 2001 11:19:12 PDT*

My humblest apologies for letting the 2600 Pennsylvania Avenue item slip by my usually more alert moderation. Moderation in the defense of moderation is no virtue, and I should have caught that one.

However, perhaps we can consider the episode a successful test of your collected readership alertness. In the entire history of the

Risks Forum,  
we have never had the volume of responses from you all that Tramm Hudson's contribution received, and thus it seemed appropriate to put out this one-item issue. There is also a correction note in the official archive copies at SRI and Newcastle.

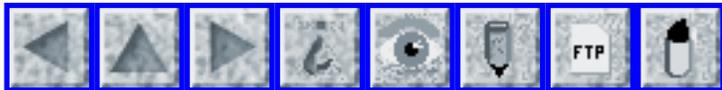
We received lots of comments about 2600 Pennsylvania Avenue \*not\* being the most famous address in the DC area, and some analyses of the actual listing for the White House at 1600 Pennsylvania Avenue. Andrew Brandt (PCWORLD) noted that the correct listing for the White House gave a Total Assessed Value: \$340,000,000, Assessed Land Value: \$314,975,600, Lot Size: 787,439 (18.1 acres), a blank ZONING field (ergo, no zoning violations there, eh?), and Property use: Special Purpose-Misc, General use: UNKNOWN.

There may have been some wonderful humorous notes as well, but I could not begin to read each of your over 100 messages. For example, one of you suggested that the author might have been the same guy responsible for the targeting error that caused the U.S. to bomb the Chinese Embassy in Yugoslavia. In addition, a few messages noted that this kind of database provides publicly available information, so what are the risks, and why are we running this in RISKS in the first place? Indeed, my relevance criterion seems to have slipped in this entire thread.

Reflecting upon all of our past issues, I am actually delighted that the Risks Forum has been so participatory. Indeed, I hope that the occasional

slip-ups on the part of our contributors -- and your moderator -- have all been rectified by subsequent postings (of which this is clearly an example). Unfortunately, the volume of submissions has increased enormously, so I am also guilty of not being able to give each and every message enough scrutiny. Consequently, your responses to errors are particularly important. If I do not get to them in a timely fashion, please resend with a suitable SUBJECT line alerting me to my possible oversight.

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 21: Issue 53**

**Thursday 19 July 2001**

## Contents

- [Dashboard can fire water at sleepy drivers](#)  
[John Arundel](#)
- [Polarized sunglasses and car LCD displays don't mix](#)  
[Henry Baker](#)
- [Missile defense test radar glitch](#)  
[PGN](#)
- [Historical Risk: KORD, and N-1 Engine Failures](#)  
[Ami Abraham Silberman](#)
- [Software gives erroneous air navigation reading](#)  
[Bill Hopkins](#)
- [Even a fatal error can't kill it](#)  
[Jim Haynes](#)
- [Gaffe gives away minister's secrets](#)  
[Paul Cornish](#)
- [SSL encryption that isn't](#)  
[Ron](#)
- [FBI arrests Russian hacker visiting U.S. for alleged DMCA breach](#)  
[Declan McCullagh](#)
- [Savings Bank software upgrade goes awry](#)  
[Jonathan Kamens](#)

- [Risk when using "Cut and Paste"](#)  
[Enrique G. Sauer](#)
  - [Re: The computer is taking over the train](#)  
[Mark Lomas](#)
  - [Re: Unexpected network congestion: remote consequences of Seti@Home](#)  
[Eric J. Korpela](#)
  - [Re: "It's public data, so why not a public database"?](#)  
[Geoff Kuenning](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

## ⚡ Dashboard can fire water at sleepy drivers

John Arundel <[john@splange.freemove.co.uk](mailto:john@splange.freemove.co.uk)>

*Thu, 19 Jul 2001 16:35:48 +0100*

Annova notes an IBM system to stop drivers falling asleep at the wheel. It asks you questions and if you fail to respond promptly, it shoots a jet of cold water over you. [http://www.ananova.com/news/story/sm\\_355015.html](http://www.ananova.com/news/story/sm_355015.html)

In the time-honoured phrase, "the RISKS are obvious". I wouldn't like to imagine the consequences if a driver was unexpectedly soaked with ice water during a high-speed overtaking manoeuvre on a motorway...

[FORDing the flood? CHEVY to the levee? NOVAcaine mutiny? PGN]

---

## ⚡ Polarized sunglasses and car LCD displays don't mix

Henry Baker <[hbaker1@pipeline.com](mailto:hbaker1@pipeline.com)>

*Wed, 18 Jul 2001 19:16:25 -0700*

I just got some new (linearly polarized) sunglasses, and got an unpleasant surprise -- I can't read the LCD displays on either my car or my wife's car without cocking my head to one side! On my car, I have to cock my head to one side by about 15 degrees, while with my wife's car I have to cock my head to the other side by about 40 degrees.

Luckily, the same angle of cocking seems to work for all of the LCD gauges at the same time.

(I just tested my sunglasses on my laptop, and I have to cock my head left by 45 degrees to get the brightest image.)

Considering the fact that polarized sunglasses are often better than unpolarized sunglasses, because they do a better job of filtering out glare (highly likely to be polarized), we actually have one safety item interfering with another.

Why can't car manufacturers install LCD's in such a manner that the polarization is compatible with polarized sunglasses?

Henry Baker <hbaker1@pipeline.com>

[We all hope you do not go off half-cocked. This reminds us of the problem of pilots on Viagra seeing various colors (including green) as blue. Blue who? PGN]

## ✦ Missile defense test radar glitch

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

*Tue, 17 Jul 2001 22:16:19 -0700 (PDT)*

The missile defense test on 14 Jul 2001 was declared a success. However, the Pentagon initially failed to note that the prototype radar had actually indicated that the interceptor had missed the dummy warhead. This omission was considered unimportant because the glitch was a minor computer programming error that could easily be fixed in time for the next test. Is that reassuring to RISKS readers?

<http://www.latimes.com/news/nationworld/nation/la-071801missile.story>

---

## ✦ Historical Risk: KORD, and N-1 Engine Failures

Ami Abraham Silberman <silber@mitre.org>

*Tue, 17 Jul 2001 10:50:19 -0400*

The following is forwarded with permission of the author, Patrick Flannery <flanner@daktel.com>. It originally appeared in sci.space.history

The N-1 was the Soviet equivalent to the U.S. Saturn V, it was to have launched the first Soviet manned lunar missions. It used a cluster of 32 rocket engines on the first stage. To handle automatic shutdown in case of emergency or failure, they used an automatic system named KORD.  
- Ami

Silberman (silber@hotmail.com)

What KORD was designed to do, and what KORD did, in detail: KORD was designed to shut down a maximum of four motors on the first stage- i.e. two malfunctioning motors, and the two motors 180 degrees opposite of them; and increase burn time of the affected stage to compensate; if more than four motors needed to be shut down, then KORD shuts all motors down. (On the second stage KORD would shut down a maximum of two motors of the eight, in the same way. On the third, four engined stage, only the defective motor was shut down, and the other three gimballed to compensate.) This would have been good for an on-pad abort during motor startup, and could have saved the rocket.....But:

Flight #1 Feb.21,1969- Within seconds of liftoff, two of the first stage motors (#12&24) were shut down erroneously by KORD; the flight continued, but at 66 seconds a Lox line ruptured, starting a fire, and KORD shut the stage down at 70 seconds, and fired the escape tower on the spacecraft successfully! Go KORD! KORD had begun to work it's "special" magic....

Flight #2 July 3rd, 1969- Day of The Big Fireworks- Almost immediately on ignition, motor #8 eats something-a bolt, welding slag, temperature sensor- stories vary; the result doesn't- turbopump blades come flying out of the housing like bullets, and sever electrical lines, and fuel and oxidizer lines on nearby engines, starting a large fire in the base of the first

stage. At only a few hundred feet altitude, KORD attempts to shut down all motors...and is 29/30ths successful in this endeavor, leaving one motor running, to neatly tip the booster 90 degrees before impact on, and destruction of, it's launch pad. The escape tower is again fired successfully! Go KORD! Some stories state that another N-1, on the other pad, gets caught in the ensuing explosion's shock waves, and has to be scrapped.

Flight #3 June 27,1971- With preternatural cunning, the Soviets have decided that it might be wise to PLAN for having the N-1 fail, and have programmed in a maneuver to get it clear of the launch pad immediately after liftoff- this maneuver is performed- and promptly overstresses the airframe, and control system, causing the rocket to fall apart in midair, and crash- but it does NOT crash on the launchpad- Success! KORD dutifully shuts down the first stage motors... a while after the third stage, and lunar spacecraft assembly, have already fallen off. The escape tower? Comrade, it was a mock-up. Boom.

Flight #4 Nov.23, 1973-With an augmented control system to allow it to do the pad clearing maneuver before it explodes, the N-1 once again vaults skyward...and keeps on going! Fifty seconds- all systems go!! 70 seconds-still go!!! 90 seconds- shut down of the center six motors, as planned!!!! 95 seconds- the center six motors are now on fire!!!!!! 110 seconds-Boom. But the escape system worked! Go KORD! Later it is discovered that if KORD had shut down the first stage motors

when the trouble started, and fired the second stage at that time, then the mission would have reached orbit. Go KORD! This then, was the apex of Soviet 1960's electronic...or at least electric, design- a safety system that both causes, and worsens, disasters. Who says we can learn nothing from Soviet spacecraft design? The KGB wants to know, comrade...who specifically said that; and what's their address?

The MITRE Corporation;W078 - C2 Systems Architecture and Integration  
12 Christopher Way;Eatontown;New Jersey;07724 (732)578-6645

---

## **✶ Software gives erroneous air navigation reading**

"Bill Hopkins" <whopkins@wmi.com>  
*Mon, 16 Jul 2001 19:32:50 -0400*

AVweb (www.avweb.com), a news service for general aviation, reported July 9 that the FAA has issued an Emergency Airworthiness Directive (AD) on one model of Apollo NAV/COM (a combined navigation and communication radio) with a specific DSP Software Version Number, because its bearing indication was found to be off by as much as 14 degrees. The Emergency AD prohibits any flight in an aircraft equipped with the radio until it is marked "Use ... for navigation prohibited."

The navigation function relies on special ground stations that (simplifying a bunch) transmit a signal that varies the phase of the

modulation with azimuth, allowing the radio to infer its bearing from a station within a degree or two. An aircraft flying a circle around a station sees the modulation change smoothly.

For many aircraft, this is the primary navigation system when flying by instruments, in clouds. Fifty miles out and 14 degrees off could put you in conflict with FAA airspace rules (bad, takes explaining) or mountains (worse, takes a funeral). In comparison, suddenly not being able to fly by instruments doesn't look so bad.

The AD text suggests that some stations do not adhere to the nominal 30 Hz modulation frequency, but the DSP software depends on the assumption that they do. I would guess that bench-testing was done only with nominal generated signals, and certification flight testing (if needed) only with stations that happened to be nominal. So, no problems showed up until a technician happened to test a new installation in the presence of a non-standard signal.

Risks: assuming, testing within assumptions, having software in the gauges, etc.

Bill Hopkins (whopkins@cacdsp.com)

[We need a too-fazed commit with 14 degrees of separation.  
PGN]

## ✶ Even a fatal error can't kill it

<jhaynes@alumni.uark.edu>

Mon, 16 Jul 2001 23:58:01 -0500 (CDT)

or "night of the living dead"

I just made an airline reservation using the web page. When I got all the way to the end, having put in the credit card information, it said "Fatal error in backend" and gave an error number and dumped me out. So I assumed (foolish assumption) that the thing had failed and started all over. The second time everything worked as it should. Then I read my email and found I had email confirmations for both of the reservations.

So I called the airline and got connected to a tech support person and he said yep, I've got two reservations on the same flight and he would cancel one of them and they would issue a refund to my credit card for it. He said the software is supposed to catch cases of the same person making two reservations on the same flight but in this case that didn't work either.

For me, this is a case of deja vu all over again. Some ten or more years ago I reported using an online banking money transfer system where I put in all the data and then the computer voice said "system error, session terminated" So I put the transaction in a few more times over the space of a few days, until I got the normal "data accepted, thank you" message. And soon after got a call from the bank about the account being

way  
overdrawn, because in fact each of the transactions had gone  
through.

No doubt there are other systems out there which have the  
possibility of  
completing a transaction and then telling the user that there  
has been a  
fatal error. Maybe a whole lot of them.

---

## **⚡ Gaffe gives away minister's secrets**

Paul Cornish <paul.cornish@psion.net>

*Tue, 17 Jul 2001 10:03:53 +0000*

A series of government initiatives have been accidentally made  
public after  
the "wrong" version of a speech by cabinet minister Stephen  
Byers was  
released. Civil servants unintentionally circulated an  
electronic copy to  
interested bodies which can be opened to reveal which passages  
have been  
removed or added during drafting. For more information see  
The Guardian Newspaper, Society Section, Thursday July 12, 2001.  
<http://www.guardian.co.uk/Archive/Article/0,4273,4220335,00.htm>

Paul Cornish <Paul.cornish@psion.net>

---

## **⚡ SSL encryption that isn't**

Ron <ron1@stop.mail-abuse.org>

*Tue, 19 Jun 2001 10:02:51 -0400*

If you submit your information to an SSL protected web page you're protected, right? Not always.

Check the EAA (Experimental Aircraft Association) web page that lets you join online. You can find it at <https://secure.eaa.org/EaaJoin/securejoin.html>

It looks good, and the browser indicates that it's 128-bit encryption. It inspires confidence until you look at the page source. Here's a couple of relevant lines [NOTE: I've modified the Email address to avoid spambots]:

```
form METHOD="POST" ACTION="..\send_email.asp"
input type="hidden" name="EMAILTO" value="joineaa@example.com"
```

It certainly appears that this 128-bit encrypted SSL form proceeds to send out your sensitive information via Email in cleartext. I verified this by modifying the form to send mail to me. I then tried it. Sure enough, the entire form is sent in clear, including credit card number.

[ADDED NOTE, 17 Jul 2001: I notified the site owner at the same time I mailed RISKS. The site is still unchanged. Ron]

---

## **⚡ FBI arrests Russian hacker visiting U.S. for alleged DMCA breach**

Declan McCullagh <[declan@well.com](mailto:declan@well.com)>  
*Tue, 17 Jul 2001 10:57:48 -0400*

Russian Adobe Hacker Busted  
By Declan McCullagh ([declan@wired.com](mailto:declan@wired.com)), 17 Jul 2001

<http://www.wired.com/news/politics/0,1283,45298,00.html>

LAS VEGAS -- FBI agents have arrested a Russian programmer for giving away software that removes the restrictions on encrypted Adobe Acrobat files. Dmitry Sklyarov, a lead programmer for Russian software company ElcomSoft, was visiting the United States for the annual Defcon hacker convention, where he gave a talk on the often-flawed security of e-books. This would be the second known prosecution under the criminal sections of the controversial Digital Millennium Copyright Act, (DMCA) which took effect last year and makes it a crime to "manufacture" products that circumvent copy protection safeguards. [...]

POLITECH -- Declan McCullagh's politics and technology mailing list

You may redistribute this message freely if you include this notice.

To subscribe, visit <http://www.politechbot.com/info/subscribe.html>

This message is archived at <http://www.politechbot.com/>

---

## **✶ Savings Bank software upgrade goes awry**

Jonathan Kamens <jik@kamens.brookline.ma.us>

*Mon, 16 Jul 2001 23:05:46 -0400*

My bank, Peoples Federal Savings Bank in Brighton, Massachusetts, "upgraded" its computer software on the weekend of June 9. No explanation of the purpose of this upgrade or description of the changes customers might see as

a result of it was distributed, either before or after the upgrade). The only notice given was a few signs posted at the bank, stating that the bank would be closed over the weekend for the upgrade.

To say that the upgrade went poorly would, from my point of view, be a huge understatement. Here's some of what went wrong (but, alas, not all of it; I'm omitting some of the minor screw-ups):

- \* All customers' telephone-banking (TB) PINs were reset as part of the upgrade.

As I noted previously, customers were not informed about this in advance.

- \* The new, default TB PIN chosen for all customers is the last four digits of the primary account holder's social security number. I'm sure I don't have to go into how monumentally stupid this is from a security point of view, especially considering that many Massachusetts residents have their social security numbers on their driver's licenses.

- \* Since the upgrade, the TB system tells you to enter the last four digits of your SSN as your PIN if this is your first time using the system, or your the PIN you've selected otherwise. However:

- \* It doesn't make it clear to previous customers of the bank that "the system" means the new TB system after the upgrade, i.e., that PINs set in the old TB system were no longer valid. You just had to figure that out by trial and error.

- \* The system doesn't force you to change your PIN from the default to

something else. So the "if this is your first time using the system"

prompt is completely wrong, since the PIN will remain the default until you

navigate about three levels deep in obscure menus to change it. And I'm

sure I don't have to go into how monumentally stupid it is from a security

point of view that the system doesn't make people change the default PIN.

\* When you requested a transfer in the old TB system and it read the

information back to you for confirmation before performing the transfer, it

read the amount of the transfer first, followed by the account numbers. This

is logical, considering that (a) the amount of the transfer is the item most

likely to have been entered incorrectly and (b) the account numbers have

already been verified as valid by the system. The new system, on the other

hand, reads both the "from" and "to" account numbers first, v-e-r-y

s-l-o-w-l-y, before reading the amount of the transfer.

\* The old TB system's transfer confirmation numbers were eight digits long,

which was already pushing it. The new system's confirmation numbers are ten

digits long. There is no excuse for forcing people to write down random

strings of ten digits which could just as easily have been half that length

if the UI had been designed properly.

\* I can no longer access my money market account from SUM ATM machines (see

[www.sum-atm.com](http://www.sum-atm.com)) run by banks other than Peoples. Before the upgrade, my

money market account was accessible as my "savings" account from these ATMs.

\* Before the upgrade my money market account was also accessible as a "savings" account from Peoples ATMs. Now, however, People's ATMs think that my money market account is a "checking" account, which means that I have two checking accounts. Therefore, when I need to access my money market account, I select "checking" and get a menu to choose which checking account I want. The menu looks like this:

1. CHECKING
2. CHECKING

That makes it intuitively obvious which one to select, eh? I had to figure out through trial and error that "1" is my old checking account and "2" is my money market account.

\* That same menu screen tells me to press Enter after using the keypad to indicate which account I want to access. But Enter doesn't work -- it gives the low "error beep." I had to figure out by trial and error that when they say "Enter", what they really mean is "the unlabeled button at the bottom of the column of buttons to the right of the screen."

\* When I made a deposit shortly after the conversion, the printed receipt for the deposit showed the same amount for both "balance" and "available balance," even though the deposit I had just made was supposed to show up immediately in "available balance" (that's how the system behaved before the upgrade). I complained to the bank about this through their Web site (well, actually, I complained to the bank about *\*all\** the problems

listed above, but

this is the only one about which they responded), and I got back a pointless

E-mail message from the bank's Operations Officer describing to me how the

system was supposed to work (which is what I had just described to him in my

complaint). I wrote back to him and emphasized again that the system was

\*not\* working that way, and he never responded.

However, two days later when I made another deposit, \*no\* balances showed up

on the receipt. Shortly after that, when I made another deposit, the

balances were back and the "available balance" correctly reflected the

deposit I had just made. So it would seem that the bank is capable of

correcting these problems, albeit not acknowledging and apologizing for them.

\* When my first statement after the upgrade arrived, I saw that I had been

charged a \$.75 ATM fee, even though I had only used Peoples and SUM ATMs all

month, and those are supposed to be free. When I called the bank about this,

I was informed that "everyone was charge 75 cents because the upgrade messed

everything up," and that the 75 cents would be credited back to my account in

my next statement. We'll see.

\* Before the upgrade, they sent out a final statement under the old system with

a closing date of June 8. No interest was paid on that statement. After the

upgrade, the next statement they sent out closed on June 30. The interest

paid out in that statement correctly covered the period of the previous

statement (i.e., they paid about 30 days of interest instead

of 22).

However, the average daily balance used to calculate the interest payment

took into account only daily balances from June 9 through June 30.

In other words, the bank underpaid interest to any customers whose average

daily balance was higher June 1-8 than it was June 9-30. Of course,

conversely, the bank paid extra interest to customers whose averages were

lower before the upgrade, but that doesn't help the customers who were

underpaid.

As I'm sure you can imagine, after this debacle I'm not too keen on continuing

to patronize Peoples. However, my fear is that when I look for alternatives,

I'm going to discover that there isn't anybody better.

Jonathan Kamens

---

## **⚡ Risk when using "Cut and Paste"**

esauer <enrique.g.sauer@lmco.com>

*Wed, 18 Jul 2001 10:30:48 +0000 (GMT)*

I just became aware of a serious security risk involving the combined use of

WinWord and Excel in Office 2000.

While writing a report in WinWord, I incorporated a graph generated via

Excel via "cut and paste". Later on, using a different computer, I decided

to edit the title of the graph by double clicking on it. To my dismay, the

\*entire\* content of the Excel file which was not residing in the computer where I was doing the editing, became available to me.

Say you have the unclassified "Graph 1" in sheet 1 of an Excel file and the classified "Graph 2" in sheet 2 of the same file. When you incorporate Graph 1 in the unclassified portion of your report you are inadvertently making Graph 2 available to the user.

To avoid this problem use "paste special", you will not be able to edit your graphs by double clicking on it, but you will avoid potentially embarrassing situations.

---

## **⚡ Re: The computer is taking over the train (Cohen, [RISKS-21.51](#))**

"Mark Lomas" <mark.lomas@tmalomas.com>

*Tue, 17 Jul 2001 12:39:15 +0100*

I am reminded of a journey on Thameslink (for those outside the UK, this company runs trains between Bedford and Brighton via London). The driver decided to brake suddenly - I don't know why, however I remember his subsequent announcement to passengers: "You may be wondering why we have to wait here. This train is fitted with a safety system which prevents the driver from accelerating following sudden braking. The computer will give me back control of the train in another minute".

This is probably a sensible (but not infallible) safety

precaution.

Mark Lomas <r21.51@absent-minded.com>

---

## **Re: Unexpected network congestion: remote consequences of Seti@Home**

"Eric J. Korpela" <korpela@ellie.ssl.berkeley.edu>

*Tue, 19 Jun 2001 18:39:47 -0700 (PDT)*

> The article closes by saying the problem was "solved" by  
> increasing the  
> number of available NAT addresses, although of course that  
> didn't fix the  
> problem, merely caused it to 'go away'. A real solution would  
> be to have the  
> screen-saver software implement incremental backoff and other  
> mechanisms  
> designed to gracefully handle a complete loss of remote server  
> access.  
>  
> One would hope that the authors of the next generation of  
> distributed  
> computation applications take heed of the lessons of the  
> current batch.

One of the risks of developing any software is that problems  
experienced by  
users will be associated with the design of the software, not  
the failure of  
other components. The GUI version of SETI@home, upon connection  
failure,  
retries the connection twice at 45 second intervals. After the  
third  
failure the program waits 60 minutes before retrying. The UNIX  
version  
waits 60 minutes between connection failures. Apart from this  
report, I am

unaware of any TCP/IP implementation that is unable to support 3  
connection  
attempts per hour.

That each computer involved ended up with 10 NAT translations  
meant that the  
router was maintaining NAT translation for failed connections  
for 120  
minutes or more. The router apparently releases translations  
promptly when  
connections succeed, but maintains them when connections fail.  
I'm not sure  
that the SETI@home software could have anticipated that.

There is another possibility. Many SETI@home users use "work  
unit" caching  
software to contact the server. We don't have much control over  
the coding  
standards used by developers of third party software that  
interacts with  
SETI@home.

Eric Korpela <SETI@home>

---

## **Re: "It's public data, so why not a public database"?**

Geoff Kuenning <geoff@cs.hmc.edu>

*Tue, 17 Jul 2001 14:21:52 -0700*

In the recent flap over 2600/1600 Pennsylvania Avenue, some  
readers  
have pointed out:

> this kind of database provides publicly available information,  
so what are  
> the risks, and why are we running this in RISKS in the first  
place?

PGN's relevance criteria did not slip up on this one. It has

often been noted in RISKS that a difference in quality is a difference in kind.

In the current example, accessing the information in the databases once required physical travel to a number of different locations, laborious removal of heavy books from shelves, and endless page-turning to locate the desired data. These physical barriers served to winnow out all but the most motivated people, mostly those who had a legitimate need.

Placing the same information online, in an easily correlated fashion, has many advantages for legitimate users, not the least of which is the elimination of the necessity of breathing dust. But it also provides new opportunities to the illegitimate. It is suddenly easy to produce lists of property owned by the wealthy, the elderly, or the vulnerable. I am not a criminal, so my creativity in this area is limited. But I recognize that there are new RISKS caused simply by changing the method of access to the database.

The foregoing is not intended to be an immovable argument against placing such databases online. We must weigh the advantages against the drawbacks.

But it is incorrect to claim that there are no RISKS issues. -- Geoff

Kuenning geoff@cs.hmc.edu <http://www.cs.hmc.edu/~geoff/>

In any large population, there are some people who aren't very bright.

That's not their fault, it's just in their genes. As an engineer, I have a responsibility to design things that won't kill off the slower

ones, just as

I have a responsibility to design things that won't harm my neighbor's dog.



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 21: Issue 54

Monday 23 July 2001

## Contents

- [Tunnel fire derails Internet service](#)  
[NewsScan](#)
- [Calendar software and departed employee](#)  
[Lawrence Kestenbaum](#)
- [U.S. Tax refund inspires Home Depot snail-mail spam](#)  
[Dawn Cohen](#)
- [Renewal of digital certificate impeded by secure passphrase](#)  
[Philip Bragg](#)
- [Security system update leads to insecurity](#)  
[Bob Van Cleef](#)
- [Did download failures increase Code Red's success?](#)  
[Scott Renfro](#)
- ["This e-mail doesn't contain any viruses"](#)  
[Aaro J Koskinen](#)
- [The risks of moving and identity theft](#)  
[Harry Erwin](#)
- [Concerns for identity theft are often unheeded](#)  
[Monty Solomon](#)
- [What a gas!](#)  
[William Paul Fiefer](#)

- ["Know Your Customer" USPS style](#)  
[Alex Wexelblat](#)
  - [US Airways credit-card snafu](#)  
[Jed Graef](#)
  - [Bad domain name?](#)  
[Gene Wirchenko](#)
  - [Banking and Internet broadcast technologies](#)  
[Daniel Chalef](#)
  - [Re: Polarized sunglasses and LCD frustration](#)  
[Stephen A. Boyd](#)
  - [Re: Even a fatal error can't kill it](#)  
[Phil Anderson](#)
  - [Re: SSL encryption that isn't](#)  
[Jacob Ofir](#)
  - [MSN security upgrade forces new e-mail address](#)  
[Ami A. Silberman](#)
  - [ISW-2001 - Call for Participation](#)  
[Howard Lipson](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

## 🔥 Tunnel fire derails Internet service

"NewsScan" <newsscan@newsscan.com>  
*Fri, 20 Jul 2001 08:52:50 -0700*

Derailed train cars burning in a Baltimore tunnel have seriously damaged the area's fiber-optic cables, slowing Internet service and other communications traffic in the Mid-Atlantic states, with a ripple effect across the country. WorldCom, PSINet and AboveNet all reported problems with service, but said they had not yet been able to quantify the severity of the problems. Keynote Systems, which measures Web site performance,

said the delay experienced by Internet users was the worst it has ever seen. "What we're seeing is a problem in the handshake between the backbones which serve as the Internet's infrastructure," said a Keynote spokeswoman. "These backbone providers hand off traffic to travel between them across the country." Keynote reported major slowdowns as far away as Seattle and Los Angeles that may be attributable to the train wreck [or Code Red? The fumes also resulted in cancellation of Orioles games. PGN]. [AP Jul 19 2001 <http://news.excite.com/news/ap/010719/18/train-derailment-communications> NewsScan Daily, 20 July 2001]

---

## **✶ Calendar software and departed employee**

Lawrence Kestenbaum <polygon@potifos.com>  
*Mon, 23 Jul 2001 14:31:52 -0400 (EDT)*

Calendaring software plays a critical role in any sizeable organization. Local governments, in particular, hold innumerable meetings -- formal meetings of the local legislative body, of course, but also committee meetings, citizen board meetings, project meetings, and on and on. And many of those meetings involve members of the public, or officials external to the organization.

The county government here in Washtenaw County, Michigan (county seat: Ann

Arbor), has about 1,300 employees. Most or all county departments use Netscape Calendar version 4.6 to schedule and keep track of meetings.

One particular county department, the Drain Commissioner's office (responsible for construction and maintenance of storm sewers and ditches all over the county) holds many meetings with local officials and property owners to discuss proposed or pending drain projects. A specific employee was responsible for putting these meetings on the calendar.

A few weeks ago, this employee left the County's employment, and her account was deleted from the system. Here's the problem: all of the many meetings she had scheduled ALSO disappeared.

As a direct result, the Drain Commissioner and other county officials, who relied on the automated calendar, were not in attendance at meetings where they were expected, resulting in inconvenience for the public and embarrassment for the officials and the County. Only then was this problem discovered. The number of future meetings that had also been lost was unknown.

I asked if the deleted meetings could be retrieved from backups. Nope, individual calendars cannot be restored, only the entire system, which obviously would disrupt over a thousand individual calendars.

The RISK: calendaring software that doesn't recognize (1) the likelihood of turnover among employees, including meeting schedulers, (2) that there are more stakeholders in a meeting than just the one person who adds it to

the official calendar, and (3) that access to information in backups may be needed on a less than all-or-nothing basis.

Lawrence Kestenbaum, polygon@potifos.com, Washtenaw County Commissioner,  
4th District, Mailing address: P.O. Box 2563, Ann Arbor MI 48106  
The Political Graveyard, <http://politicalgraveyard.com>

---

## **⚡ U.S. Tax refund inspires Home Depot snail-mail spam**

"Dawn Cohen" <COHEND@war.wyeth.com>  
*Mon, 23 Jul 2001 10:08:36 -0400*

Bloomberg radio reports that Home Depot will do a targeted mailing synchronized with tax refunds. Apparently the tax refunds are being sent out in an order related to the Social Security Number (I think it may be just the last 2 digits). Home Depot has SSN information for a number of their customers (I believe those with Home Depot cards). So they will send out advertising flyers to their customers in the SSN order, timed to be viewed just when the customer needs help deciding what do with the refund check.

---

## **⚡ Renewal of digital certificate impeded by secure passphrase**

<philip.bragg@technocom.com>  
*Fri, 20 Jul 2001 16:42:09 +0100*

I work for a company which had purchased a digital certificate from BT Trustwise (now part of Ignite) 12 months ago, I now find that I am unable to renew it online.

The problem is the "log in" passphrase contains some non-alphanumeric characters, this is a practice which would surely meet with industry-wide approval as it makes brute force attacks more difficult. At the time of purchase the BT Trustwise system accepted the passphrase and duly created and delivered a working certificate.

Today the Web page where new passphrases are entered has a warning telling customers to use alphanumeric characters only, whether it stops users entering anything else is unknown at this time. I am told by the person who originally created the certificate that no such warning was displayed at the time of purchase.

The software which processes the online renewals malfunctions if it sees anything but alphanumeric characters in an existing user's passphrase. It is possible to determine that the passphrase is being recognised as valid because after entering it correctly I get delivered to a mostly blank and useless page, entering something which isn't my passphrase takes me to a page telling me my passphrase is incorrect.

If the system knows I am using the correct passphrase why won't it let me renew my certificate?

It seems to me that Trustwise is covering up a minor programming error with a simple message saying "don't do this or it will break" rather than fixing the problem, something I find quite surprising given the business they're in.

The risk of having no valid certificate became a different risk, that of having an insecure certificate, when the support person at the company concerned offered to enter the passphrase directly into their system if I read it over the phone to them.

Then there is the risk of overlooking directions to use only insecure passwords...

Philip Bragg

---

## **✶ Security system update leads to insecurity**

Bob Van Cleef <vancleef@garg.com>

*Mon, 23 Jul 2001 10:41:20 -0700 (PDT)*

The security service that monitors the building where I work recently upgraded its alarm monitoring software. The people from their corporate office arrived, installed the upgrade, and left...

Unfortunately, while they were here, they appear to have also deleted the configuration database and all backups... as the local people ended up manually re-entering all the system settings, for all their clients, by

hand.

A month later our computer room air-conditioning went out and the over-temperature alarm did not go off. They forgot to tell the computer to monitor that line. Fortunately one of our staff walked into the room before damage was done. (Our manual backup sensor.)

They tell me that everything is now working correctly. Why am I still nervous?

Bob Van Cleef, San Jose, CA [www.garg.com](http://www.garg.com)

---

## ⚡ Did download failures increase Code Red's success?

Scott Renfro <[scott@renfro.org](mailto:scott@renfro.org)>

*Sun, 22 Jul 2001 18:43:09 -0700*

[For those of you who slept through it, the Code Red worm was intended to attack the [whitehouse.gov](http://whitehouse.gov) Web site at 5pm EDT on 19 Jul 2001. With just-in-time reverse engineering, the code was discovered to contain the target IP address, thus enabling the White House staff to reconfigure to avoid the attack. (The attack clearly could have been more subtle.) It is of course ironic that current efforts to outlaw reverse engineering (DMCA, UCITA, etc.) could ban efforts to stave off this and other attacks! The relevant CERT advisory is at <http://www.cert.org/advisories/CA-2001-19.html> pointing out that Code Red exploited a vulnerability noted earlier in CA-2001-13. YABO:

Yet Another

Buffer Overflow, aimed at Microsoft IIS servers. PGN]

On the morning of 19 Jul 2001, I notified a small company (whom I sometimes advise since they have no dedicated IT staff) of the then-latest Microsoft advisory. An hour later, they proudly replied, reporting success and noting that this hot fix was much easier to apply than most -- especially since this one didn't force a reboot.

Suspicious that they hadn't really applied the hot fix, I downloaded a separate copy of the hot fix using Internet Explorer and sent it to them via e-mail. This time they replied that the attachment I sent resulted in an error message: 'not a valid Windows NT application.'

I soon realized that the connections were terminating prior to completion and Internet Explorer was not reporting the failures. In the user's mind, silence was equivalent to success.

We were able to successfully download the hot fix using wget on FreeBSD, which restarted the transfer four times due to reset connections -- each time picking up where it had previously left off. The company's server was soon patched, and they have had no problems with the Code Red worm.

I've confirmed that Internet Explorer 5.0 on Win2k reports no failures in (at least) the following situations:

- When the user has selected 'Run this program from its current location' and the connection is prematurely reset, the download dialog silently disappears. This is the same visual behavior

as a

program that was successfully transferred and completed execution

without pausing for user input.

- When the user has selected 'Save this program to disk' and the connection is closed normally but prematurely (i.e., before the

number of bytes specified in the Content-Length header were received), the total file size is silently changed. For example,

during the download, the dialog displays:

Estimated time left: 2 sec (87.2 KB of 236 KB copied)

but once the connection has closed, the dialog changes to:

Downloaded: 180 KB in 1 sec

An error does result in the inverse of these situations (i.e., when running

a program where the connection is closed normally but prematurely or when

saving a program where the connection is reset).

One wonders how many naive admins thought they \*had\* installed the hot fix,

but ended up with a truncated download and a Code Red worm infestation

instead.

P.S. As of 22 Jul 2001, transfers from [mssjus.www.conxion.com](http://mssjus.www.conxion.com) (to which

[download.microsoft.com](http://download.microsoft.com) at least sometimes redirects) still result in

frequent resets from some networks.

---

**✶ "This e-mail doesn't contain any viruses"**

Aaro J Koskinen <[akoskine@cc.helsinki.fi](mailto:akoskine@cc.helsinki.fi)>

*Mon, 23 Jul 2001 16:59:02 +0300 (EET DST)*

I recently received e-mail from a stranger with the following note at the end:

> This message has been scanned for viruses with F-Secure Anti-Virus for  
> Microsoft Exchange and it has been found clean.

RISKS: Someone could actually take such a note for real and blindly trust it!

There is no way to tell whether any scanning has been actually done. I might as well add a similar note to my .signature! Secondly, who would trust virus scanning done by the \*sender\* anyway?

Aaro Koskinen, aaro@iki.fi, <http://www.iki.fi/aaro>

---

## **⚡ The risks of moving and identity theft**

Harry Erwin <harry.erwin@sunderland.ac.uk>

*Mon, 23 Jul 2001 18:08:04 +0100*

In January 2001, I moved to the UK to take up a position as a Senior Lecturer of Computing at the University of Sunderland in the UK. Today, I got the first bill for a credit card taken out fraudulently in my name back in the US. I was fairly careful about these things -- I suspect this is the tip of the iceberg.

The first step, of course, was to file fraud alerts with the three major credit bureaus. Trans Union was very helpful, and even indicated that the incident I already knew about was the only one on my recent

record.

Experian was not as helpful -- I had to provide an obsolete ZIP code to reach the point of actually filing the data they needed, but then they recorded my voice as I provided the rest. Equifax was hopeless. They couldn't handle (UK) rotary phones, and they required a US phone number for contact purposes. They also had problems reading my SSN, and they finally ejected me from the system, requesting a letter with about five pages of miscellaneous details, some of which (a pay stub with my SSN) are simply not available in the UK. I filed a complaint on that with the FTC. Next step is a letter to the credit-card issuer to follow up on my voice report. I suspect my notary will be busy.

Harry Erwin, University of Sunderland. Computational neuroscientist modeling bat bioacoustics and behavior. <<http://world.std.com/~herwin>>

---

## **⚡ Concerns for identity theft are often unheeded**

Monty Solomon <monty@roscom.com>

*Mon, 23 Jul 2001 14:58:15 -0400*

Major financial institutions routinely give out confidential customer account information to callers, using security procedures that authorities say are vulnerable to abuse by fraud artists. Regulators and law enforcement officials warned three years ago that identity thieves and

information brokers were tricking clerks into giving them access to individuals' financial information. [Source: Robert O'Harrow Jr., Washington Post Staff Writer, 23 Jul 2001; Page A01, <http://www.washingtonpost.com/wp-dyn/articles/A27475-2001Jul20.html>]

---

## ⚡ What a gas!

Paul <yamada@prairienet.org>  
*Mon, 23 Jul 2001 14:10:45 -0500*

I am a longtime customer in good standing with Nicor, a large natural gas utility serving portions of northern Illinois (United States). I recently had my gas shutoff, the meter locked, and the meter scheduled for removal from outside my house. Luckily I was home when the Nicor technician arrived to haul away the meter and I asked her to check the order.

Armed with a telephone and e-mail client, I discovered anyone can cut anyone else's Nicor service off by supplying either an address or telephone number. One representative told me requests for shutoff are honored immediately.

To a degree, this is understandable. Fire departments must, for example, kill the gas to a burning building. But the ease with which a cutoff under far less threatening circumstances can occur is remarkable.

To their credit, Nicor is investigating the processes in place that allow

this. Their default for each account, for example, is *\*not\** to password-protect it (that is, mother's maiden name or some such checkpoint).

Is this a software RISK? I think so. Shutoff requests are keyed into a system with under veil of the skimpiest verification. Systems with "screen pop," which display the telephone number of the caller, also act as a checkpoint. This system appears divorced from a screen pop function. In this case, the final checkpoint is an onsite technician who can only debug the problem if the homeowner happens to be in. That's the type of debugging I expect from, say Microsoft, not my utility company.

William Paul Fiefer (and please don't cut my gas off)

---

## ⚡ "Know Your Customer" USPS style

Graystreak <wex@media.mit.edu>

*Sun, 22 Jul 2001 11:00:43 -0400*

Insight Magazine reports [1] that since 1997, the US Postal Service has been reporting innocent activity it deems "suspicious" to federal law enforcement officials. Evidence includes a training video with this chilling instruction:

"It's better to report 10 legal transactions than to let one illegal transaction get by."

The risks of a system that presumes guilt until innocence is proven are too numerous to list here. Not least of them is the impossibility of proving a

negative (I did not intend this cash to be used for illegal purposes). A similar reporting system in the banking arena is known to generate ratio of 99,999 false positives for every true positive. Yes, I do mean a ratio of  $10^5:1$  errors to correct results. I can't imagine any other system in which that error rate would be acceptable.

The information on suspicious activities is, of course, kept in a database controlled in secret and used for purposes no one is willing to discuss.

The Post Office will not discuss the parameters used to flag "suspicious" activity, though the video states that unwillingness to give out personal information such as date of birth and/or produce identification papers is automatically suspicious.

Someone help me verify that I'm still living in America, please?  
[\*]

[1] <http://www.moreprivacy.com/editorials/postaleye.htm>

Alan Wexelblat <[wex@media.mit.edu](mailto:wex@media.mit.edu)> <http://wex.www.media.mit.edu/people/wex/>

CHI'02 Panels Chair, moderator, [rec.arts.sf.reviews](mailto:rec.arts.sf.reviews)

[\* Alex, Yes, you are. But privacy is continually being eroded, despite the best efforts of the Risks Forum, the Privacy Forum at <http://www.vortex.com/privacy>, EPIC at <http://www.epic.org>, EFF at <http://www.eff.org>, Zero Knowledge at <http://www.zeroknowledge.com>, to name just a few. PGN]

## ✶ US Airways credit-card snafu

"Jed Graef" <jgraef@worldnet.att.net>

*Fri, 20 Jul 2001 16:40:32 -0400*

Recently my wife needed to redeem US Airways miles for a ticket on short notice. The fee for the last minute booking was \$75, which I paid with a credit card at the airport.

When the credit-card bill came, there were two charges for the \$75. The US Air representative I spoke to cheerfully reversed one of the charges and explained that, due to a known "programming error," after the card was swiped, the record of the transaction was not cleared upon completion. When the next customer's card was swiped, the last transaction in the system (mine) was processed again, resulting in the double billing.

He explained all of this to me so that I would not be concerned about seeing someone else's name as the passenger on the confirmation letter that would be sent. Sure enough, the letter arrived with the name of the person whose card was swiped after mine.

One has to wonder how long this error has been known.

Jed Graef <jgraef@att.net>

---

## ✶ Bad domain name?

Gene Wirchenko <genew@shuswap.net>

*Fri, 20 Jul 2001 19:06:34 -0700*

I live in Salmon Arm, British Columbia, Canada. Suppose you wanted to create a Web site for promoting the downtown Salmon Arm area.

These names are a bit long:

downtownsalmonarm.bc.ca

salmonarmdowntown.bc.ca

The most common (and presumably obvious) abbreviation of the community

name is "SA". You could abbreviate -- as someone did:

sadowntown.bc.ca

Unfortunately, this can easily be lexed to:

sad own town

The risk? When mapping a name to another set of rules, watch that you aren't now saying something other than what you mean to say.

Gene Wirchenko

[This is of course a very old problem -- as in "together" vs "to get her".

With the high price of fuel, the town may be dealing with "sa gas". Perhaps

"sa les girls"? I presume the town song is "Salmon Chanted Evening". PGN]

---

## **Banking and Internet broadcast technologies**

Daniel Chalef <daniel@zoo.co.za>

*Sat, 21 Jul 2001 09:00:01 +0200*

A local Internet-based bank (a joint venture of South Africa's largest ISP and a local banking group) ran into a spot of trouble with a mass e-mailing list of a sister company, MoneyMax. MoneyMax provides online securities trading and securities-related information to the bank's customers. It appears the wires got crossed, and confidential information in response to one person's credit-card application made it onto MoneyMax's daily financial newsletter. Thankfully, somebody noticed after mailing to about 2% of the list, and pulled the plug on the mailserver. [The e-mail apology entitled "Please delete previous Moneymax Newsletter" blamed an "unforeseen software error", and included the customary "Measures have been taken to ensure that it will not happen again." PGN-ed]

---

## **★ Re: Polarized sunglasses and LCD frustration (Baker, [RISKS-21.53](#))**

Stephen A. Boyd <UncleHonus@aol.com>

*Mon, 23 Jul 2001 13:35:46 EDT*

In response to Henry Baker's aggravation, it would take a broad, concerted effort on the part of several industries to coordinate LCD screen angle with the linear polarization manufacture methods for lenses. It's my understanding that they come in sheets and their orientation is not a manufacturing concern when the sunglasses are manufactured. This answers

hbaker's wondering as to why he cocks his head at only a 15-degree angle for his wife's screen but 40 for his and 45 for his laptop. He will see this (up to a full 90 degrees) for many to most of the LCDs that are so quickly emerging as standard equipment for displays, ATMs etc.

This may be particularly RISKS relevant, since the "accutint" lenses or those that react with sunlight (UV rad.) may also react adversely, depending on the linear angle and whether it's merely arbitrary during manufacture. Imagine the risk, driving into a sunlit area (like after a tunnel or cloudcover or something). Ugh!

Stephen A. Boyd, Chief Information Officer, Premier Heart, LLC

[Re: Brewster's angle of incidence: perhaps the Brewster Rooster cocks its head cluckwise. PGN]

---

## ✶ Re: Even a fatal error can't kill it (Haynes, [RISKS-21.53](#))

<phil.anderson@amsjv.com>

*Fri, 20 Jul 2001 12:14:45 +0100*

> ... the software is supposed to catch cases of the same person making two  
> reservations on the same flight but in this case that didn't work either.

That in itself sounds risky - I was on a trip once where the group included two sisters, same surname, same initial; the hotel manager had assumed that one of the entries on the list was an erroneous duplicate and

only allocated  
one room.

Philip Anderson, Alenia Marconi Systems Cwmbrân, Cymru/Wales

---

**⚡ Re: SSL encryption that isn't (Ron, [RISKS-21.53](#))**

"Jacob Ofir" <jofir@nortelnetworks.com>

*Thu, 19 Jul 2001 19:30:18 -0400*

What the EAA Web page does is quite common. The web-browser submits the information using SSL to the server, and the server e-mails that information in cleartext to some destination. I imagine that most small "registration" pages do similar things, with the main difference being that they hard-code the destination address in the server, rather than submitting it with the form.

One risk is that users have been taught that a padlock on their browser means that everything is secure. A greater risk is that some (most?) developers believe the aforementioned statement and do not worry about the treatment of user data once it arrives at the server.

Jacob

---

**⚡ MSN security upgrade forces new e-mail address**

"Ami A. Silberman" <silber@mitre.org>

*Mon, 23 Jul 2001 09:58:44 -0400*

My home account is with MSN. A couple of years ago, my address was blahblah@msn.com. After an upgrade, it became blahblah@email.msn.com. However, I could still use the old address as a return address, and people could still send mail to me at both addresses. Since then, I've joined a couple of mailing lists, with my e-mail address as blahblah@email.msn.com.

Recently, MSN required all its users to upgrade to some new security configuration which is supposed to remove spam. (It hasn't, and for the first time I'm getting spam purporting to be from actual old e-mail address.) In the process, my e-mail address changed again back to blahblah@msn.com.

The problem is that now I can no longer post to my mailing lists, which have me as blahblah@email.msn.com. Not only that, but although I can resubscribe with my new address, I cannot unsubscribe using my old address, since the MSN servers refuse to acknowledge it. (This is probably their spam-blocking.) I'm having to pester the administrators of several lists to unsubscribe me manually. Since this is probably happening to everyone who has an msn account, the problem is non-trivial.

The risk? MSN's attempt to improve security (apparently by forcing spammers to modify their software to change fake msn addresses) has resulted in additional burden on list administrators.

Ami Silberman (ami\_silberman@hotmail.com)

---

## **ISW-2001 - Call for Participation**

Howard Lipson <hfl@cert.org>

*Fri, 20 Jul 2001 18:11:30 -0400 (EDT)*

Fourth Information Survivability Workshop (ISW-2001)

"Impediments to Achieving Survivable Systems"

<http://www.cert.org/research/isw.html>

The Delta Pinnacle Hotel

Vancouver, BC Canada

October 15-17, 2001

Sponsored by the IEEE Computer Society and the US State  
Department

With support from the Government of Canada

Organized by the CERT\* Coordination Center, Software Engineering  
Institute

General Chair: John McHugh, CERT\*/CC

Program Chair: Corey Schou, Idaho State University

Participation in the workshop is by invitation only. There are  
two ways to  
obtain an invitation:

\* Submit a position paper related to the theme of the  
workshop, by  
31 August 2001.

\* Submit a request for an invitation, accompanied by a  
qualification  
statement, by 15 September 2001.

Please see the ISW Web site for the complete call for  
participation,

including detailed instructions on submitting a position paper  
or a  
qualification statement. Check the Web site periodically for  
updates about

the workshop:

<http://www.cert.org/research/isw.html>

Please send any questions or comments about ISW-2001 to:  
[isw-2001@cert.org](mailto:isw-2001@cert.org)

\* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office. Copyright 2001 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 21: Issue 55**

**Tuesday 31 July 2001**

## Contents

- [Oxygen tank kills MRI exam subject](#)  
[PGN](#)
- [Software is called capable of copying any human voice](#)  
[PGN](#)
- [Software safeguards prevent Solar Sail from separation?](#)  
[Stanislav Shalunov](#)
- [Firefighter's phone lines disrupted because of a SMS hoax](#)  
[Stanislav Meduna](#)
- [New results on WEP](#)  
[Adi Shamir via Matt Blaze](#)
- [FBI hit with Sircam virus that distributes files on your HD](#)  
[Declan McCullagh](#)
- [Super-accurate atomic clock hates Sundays](#)  
[Ken Knowlton](#)
- [Risks of relationships online](#)  
[Gary Stock](#)
- [Apple DNS Entry hacked](#)  
[Greg Searle](#)
- [University of Pennsylvania cable cut](#)  
[Rebecca Mercuri](#)

- [Cell phones overload 911 in Denver](#)  
[Richard J. Barbalace](#)
  - [Qwest Wireless erroneously overbills customers by thousands of dollars](#)  
[Richard Kaszeta](#)
  - [Re: FBI arrests Russian hacker visiting U.S. for alleged DMCA breach](#)  
[Bill McGonigle](#)
  - [More on the risk of moving and identity theft](#)  
[Harry Erwin](#)
  - [REVIEW: Bruce Schneier, "Secrets and Lies: Digital Security in a Networked World](#)  
[Rob Slade](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

## ✶ Oxygen tank kills MRI exam subject

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

*Tue, 31 Jul 2001 10:09:32 -0700*

In New York's Westchester Medical Center on 27 Jul 2001, the head of a 6-year-old boy was severely smashed by a metal oxygen tank that had been attracted by the 10-ton electromagnet during a post-operative MRI (magnetic imaging resonance) exam. He died two days later. The exam was intended to check his progress after a benign tumor had been removed from his brain.

[Source: Child Killed in MRI Machine, by Jim Fitzgerald, Associated Press

Writer, 31 Jul 2001; PGN-ed; this article noted that in March 2001, "an

accreditation team caught the staff altering a patient's chart and

automatically gave it a ranking that was among the lowest in the country."

The article also noted that in 2000 in Rochester, NY, "an MRI magnet yanked

a .45-caliber gun out of the hand of a police officer, and the

gun shot a  
round that lodged in a wall."

[RISKS readers have long noted a tendency toward prolonged  
disregard for  
warnings of severe risks. Here is a quote on MRI risks from  
the

National Institutes of Health in 1987 (courtesy of Lauren  
Weinstein):

The National Institutes of Health stress the danger of  
leaving objects

that can be magnetized near the machine. "The most  
important known risk

is the projectile effect, which involves the forceful  
attraction of

ferromagnetic objects to the magnet," the NIH concluded  
after a

conference studying the devices in 1987.]

---

## **✶ Software is called capable of copying any human voice**

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

*Tue, 31 Jul 2001 9:57:13 PDT*

An article by Lisa Guernsey in *\*The New York Times\** on 31 Jul  
2001 notes  
that AT&T Labs will start selling a system called Natural Voices  
that turns  
printed text into speech -- seemingly in the voice of arbitrary  
individuals  
for whom the system has been tailored after analyzing something  
like 10 to  
40 hours of recordings. The results are quite remarkable in  
capturing  
personal inflections and intonations -- although by no means  
perfect.

[The technology is of course fascinating. However, it will undoubtedly lead to advertisements mimicking the voices of all sorts of famous folks. The risks of course are legion (masquerading, fraud, etc.), and raise many issues such as who owns the rights to a particular person's voice? This technology will of course further muddy the legal waters over real vs simulated characters doing nasty things.]

---

## ✶ Software safeguards prevent Solar Sail from separation?

stanislav shalunov <shalunov@internet2.edu>  
23 Jul 2001 01:48:59 -0400

It appears that the reason for failure[1] of the recent Solar Sail launch[2] from a submerged Russian submarine could have been a software bug (excerpted from [3]):

> A very preliminary examination of the rocket telemetry data in  
> Russia indicates that the separation command was terminated by an  
> on-board fail-safe program because dynamic variations were sensed in  
> the third stage. The launch vehicle was pre-programmed to override  
> the separation command in the presence of dynamic variation. These  
> variations would not have affected the Cosmos 1 test spacecraft  
> performance or its recovery. This possibility is being examined  
> further.

It is, perhaps, worth noticing that similar environment monitoring

techniques are reportedly used on some Russian ICBMs to make it harder to detonate a stolen nuclear warhead without going through a ballistic missile launch. These techniques are believed to have a generally low probability of false positives.

[1] [http://dailynews.yahoo.com/htx/ap/20010721/sc/solar\\_sail\\_4.html](http://dailynews.yahoo.com/htx/ap/20010721/sc/solar_sail_4.html)

[2] [http://dailynews.yahoo.com/htx/nm/20010720/sc/space\\_russia\\_dc\\_1.html](http://dailynews.yahoo.com/htx/nm/20010720/sc/space_russia_dc_1.html)

[3] <http://www.planetary.org/solarsail/Media.htm>

Stanislav Shalunov  
[~shalunov/](http://www.internet2.edu/~shalunov/)

<http://www.internet2.edu/>

---

## 🔥 Firefighter's phone lines disrupted because of a SMS hoax

Stanislav Meduna <stano@meduna.org>

*Sat, 21 Jul 2001 11:56:40 +0200*

Phone lines of the firefighters in all regions of Slovakia were severely overloaded for two days as tens of thousands calls were made to it.

The cause was a hoax SMS spreading in the network of one of the GSM operators stating that it is possible to make free calls using this number. The GSM operator itself also had minor problems in some areas. Despite coverage in main news the calls continued also the next day.

Many people apparently did not recognize that the number is an emergency one and blindly called it. Even more people forwarded the message to all friends without thinking of it or trying it.

Risk 1: You don't need any mail client executing scripts to spread some piece of info faster than the system is able to handle. A plain old human stupidity fully suffices and in this case endangered human lives. Don't assume that if one is intelligent enough to use services such as SMS, he/she won't respond to this kind of hoax. That particular operator has less than 700 000 customers, the number of calls made was quoted as tens of thousands. Go figure...

Risk 2: If the originator was smart enough to use web-to-SMS gateway via some anonymizer, he is practically untraceable (the individual would be facing 8 to 10 years in prison). The intent of the callers and forwarders will be much harder to prove and our justice already is overloaded enough, so they probably don't have to fear much.

---

## ✶ New results on WEP (via Matt Blaze)

Adi Shamir <shamir@wisdom.weizmann.ac.il>

*Thu, 26 Jul 2001 00:50:03 +0300*

[Matt Blaze <mab@research.att.com> sent me this item on a practical

WEP attack, and put Adi's paper at

[http://www.crypto.com/papers/others/rc4\\_ksaproc.ps](http://www.crypto.com/papers/others/rc4_ksaproc.ps)

He notes that "as far as I know WEP isn't used for copy protection,

so it's still legal to disseminate and traffic in this kind of information...

Ben Laurie <ben@algroup.co.uk> suggests that this exhibits two risks

for the price of one: (1) Expecting WEP to give you what it claims

(i.e. Wired Equivalence) is RISKing your data; (2) Doing this kind of

thing and visiting the US is RISKing your liberty. PGN]

WEP is the security protocol used in the widely deployed IEEE 802.11

wireless LAN's. This protocol received a lot of attention this year, and

several groups of researchers have described a number of ways to bypass its

security.

Attached you will find a new paper which describes a truly practical direct

attack on WEP's cryptography. It is an extremely powerful attack which can

be applied even when WEP's RC4 stream cipher uses a 2048 bit secret key (its

maximal size) and 128 bit IV modifiers (as proposed in WEP2).

The attacker

can be a completely passive eavesdropper (i.e., he does not have to inject

packets, monitor responses, or use accomplices) and thus his existence is

essentially undetectable. It is a pure known-ciphertext attack (i.e., the

attacker need not know or choose their corresponding plaintexts). After

scanning several hundred thousand packets, the attacker can completely

recover the secret key and thus decrypt all the ciphertexts. The running

time of the attack grows linearly instead of exponentially with the key

size, and thus it is negligible even for 2048 bit keys.

Adi Shamir

## **🔥 FBI hit with Sircam virus that distributes files on your HD**

Declan McCullagh <declan@well.com>

*Wed, 25 Jul 2001 18:30:09 -0400*

CERT has (ahem, finally) released a Sircam advisory this afternoon:

<http://www.cert.org/advisories/CA-2001-22.html>

Sircam is an amazingly noxious critter. I'll give you an example. At Wired News, like other news organizations, we have feedback addresses so people can send us thoughts on articles. Those have been the same for at least three years, so they're well-known and available to programs like Sircam that scan hard drives for e-mail addresses.

Since 1 am ET 24 Jul 2001, we've received about 150 MB of mail directed at those addresses, the vast bulk of it Sircam output. A quick scroll through the messages says about 90 percent of it by message and probably 99 percent of it by size is due to Sircam.

Dave Farber wrote on his Interesting People list:

> The person/group who launched the SirCam virus should get the first  
> Cyberspace death-- namely permanent banishment from any network access any  
> place in the world. We yell endlessly about spam mail but one mess like  
> this makes spam mail almost interesting.

Which I heartily endorse.

-Declan

[Declan appended Ted Bridis's \*Wall Street Journal\* item on 25

Jul 2001,

sent to him by Ted:

<http://interactive.wsj.com/articles/SB99601609210000000.htm>

The essence of that article is that the FBI's cyberprotection unit

accidentally sent private FBI documents by e-mail outside of the FBI.

It appears that this was the result of the Sircam virus infecting

an FBI internal computer. PGN-ed]

---

## **✶ Super-accurate atomic clock hates Sundays**

Ken Knowlton <KCKnowlton@aol.com>

*Sat, 28 Jul 2001 20:32:49 EDT*

The large electronic Millennium Clock display at Ottawa's National Research

Council has been losing an hour every Sunday. although the clock itself

remains accurate to within a few millionths of a second per year. The

problem appears to stem from botched software to handle the daylight savings

cutover on 1 Apr 2001. Incidentally, the display includes a plaque saying

that the Millennium Clock ``celebrates Canada's rich history of leadership

in timekeeping.'' Apparently, the display had been plagued by problems

since it was installed in June 1999 to celebrate the turn of the century,

and intended to exist only through the Y2K cutover. [Source: Reuters, 30

Apr 2001, from AOL's "News of the Weird"; PGN-ed]

[Note the unrelated Millennium clock problem reported by Mike Palmer

in [RISKS-21.20](#). PGN]

---

## ✶ Risks of relationships online

Gary Stock <gstock@unblinking.com>

*Fri, 20 Jul 2001 07:49:48 -0400*

A reminder: 'FRISKY' is just a big F-Y with 'RISK' in the middle :-)

[http://www.ananova.com/news/story/sm\\_354103.html  
?menu=news.weirdworld.rockyrelationships](http://www.ananova.com/news/story/sm_354103.html?menu=news.weirdworld.rockyrelationships)

Husband's internet date turns out to be his wife

A married couple in China ended up brawling after realising they had unwittingly courted each other over the internet.

The pair from Beijing sneaked online to flirt with their mystery girlfriend and boyfriend at a chat website called the Green, Green Schoolyard.

After a month, the man arranged to meet up with his ideal new friend only to discover it was actually his wife. He had known only her user name, I Want You.

They each agreed to carry a certain newspaper to identify themselves, but were shocked when they came face-to-face and started fighting in the street.

Passers-by eventually alerted security guards who had to separate the two, reports Norway's main news agency NTB.

Gary Stock, UnBlinking gstock@unblinking.com <http://unblinking.com/>

---

## 🔥 Apple DNS Entry hacked

"Greg Searle" <greg\_searle@hotmail.com>

*Fri, 20 Jul 2001 10:09:19 -0400*

I just happened to look up apple.com (this morning), and here is what came out:

Whois Server Version 1.3

Domain names in the .com, .net, and .org domains can now be registered with many different competing registrars. Go to <http://www.internic.net> for detailed information.

```
APPLE.COM.IS.THE.CHOICE.OF.ALL.SELF.RESPECTING.TERRORISTS.NET
APPLE.COM.IS.KRAD-NEAT.BUT.SO.IS.JIMPHILLIPS.ORG
APPLE.COM
```

To single out one record, look it up with "zzz", where zzz is one of the of the records displayed above. If the records are the same, look them up with "=zzz" to receive a full display for each record.

```
>>> Last update of whois database: Fri, 20 Jul 2001 01:56:29 EDT
<<<
```

The Registry database contains ONLY .COM, .NET, .ORG, .EDU domains and Registrars.

[Note: "x"s changed to "z"s to avoid filtering! PGN]

---

## ⚡ University of Pennsylvania cable cut

<mercuri@gradient.cis.upenn.edu>

*Mon, 23 Jul 2001 19:34:16 -0400 (EDT)*

According to the ISC Network Operations Center <noc@isc.upenn.edu>, at 5:15pm on 23 Jul 2001, more than a dozen buildings lost their network connectivity, due to a fiber cut. [The NOC-wors(h)t is yet to come? PGN-ed]

---

## ⚡ Cell phones overload 911 in Denver

"Richard J. Barbalace" <rjbarbal@MIT.EDU>

*Mon, 23 Jul 2001 12:22:36 -0400*

The \*Rocky Mountain News\* reports that Denver's 911 call centers are being overwhelmed by increasing numbers of phone calls, some of which are never answered because of staffing problems. A tragedy has not happened yet, but the story suggests this is mere luck, noting a shooting in which 911 reports were ignored. One-touch 911 buttons make calling easier. Many calls now come in to report a minor accident, instead of just a few. [PGN-ed]

Then there are the calls operators receive by accident, when someone jostles their phone in their purse, pocket or on their utility

belt.

Construction workers, in particular, often dial 911 by mistake while

leaning over guardrails to assess their work. "We can hear their entire

conversation, but they can't hear us because of all the background noise,"

Hilburn said. "This is a really common thing for us."

The risk is making it too easy for everyone to contact help in an emergency, resulting in a type of unintentional denial of service attack.

The full article is at:

[http://www.insidedenver.com/drmn/local/article/0,1299,DRMN\\_15\\_755959,00.html](http://www.insidedenver.com/drmn/local/article/0,1299,DRMN_15_755959,00.html)

Richard J. Barbalace <rjbarbal@mit.edu>

---

## **✂ Qwest Wireless erroneously overbills customers by thousands of dollars**

Richard Kaszeta <kaszeta@me.umn.edu>

*Tue, 24 Jul 2001 11:48:40 -0500 (CDT)*

According to

[http://www.startribune.com/viewers/qview/cgi/qview.cgi?template=metro\\_a&slug=qwes24](http://www.startribune.com/viewers/qview/cgi/qview.cgi?template=metro_a&slug=qwes24)

Qwest Wireless apparently had a major error in their billing software,

and appeared to be billing customers at hundreds of dollars per minute

for usage in excess of their allotted monthly limits.

Quoting the article:

One Minneapolis customer received a bill for \$57,346.20.

Some 14,000 of Qwest's wireless phone customers in 14 states were vastly overcharged, said spokesman Bryce Hallowell. The errors resulted from a glitch in a new Qwest computerized billing system. Customers whose calls exceeded the number of free minutes on their wireless calling plans were billed at excessive rates. The glitch has since been corrected.

Richard W Kaszeta <rich@kaszeta.org> <http://www.kaszeta.org/rich>

---

## **✶ Re: FBI arrests Russian hacker visiting U.S. for alleged DMCA breach**

Bill McGonigle <mcgonigle@medicalmedia.com>

*Fri, 20 Jul 2001 11:14:26 -0400*

(McCullagh, [RISKS-21.53](#))

Interesting that this one slipped through the crack without an analysis of the real risk involved here. This 'russian hacker' (or 'employee of a Russian data recovery company' some might say) did his work for a company in Russia; the company distributed their from there. As far as I know the DMCA is a US law and doesn't apply to overseas activities. Regardless, Mr. Sklyarov's activity in the US was giving a speech. The risk here is assuming a country with supposed constitutional protection for free speech won't throw you in the clink for the same (or for pissing off a US company).

## ✂ More on the risk of moving and identity theft (Re: [RISKS-21.54](#))

Harry Erwin <harry.erwin@sunderland.ac.uk>

*Fri, 27 Jul 2001 07:50:43 +0100*

The card was requested from a phone in Richmond, Virginia, after I filed a change of address with the Virginia DMV. Virginia drivers licenses have the SSN as the default identifier. Within a week, charges were being made using the fraudulent card in Florida and California.

Harry Erwin, University of Sunderland. Computational neuroscientist modeling bat bioacoustics and behavior. <<http://world.std.com/~herwin>>

[Virginia was where in 1991 DMV employees were fraudulently giving out bogus licenses. See the lead item in [RISKS-11.41](#). PGN]

---

## ✂ REVIEW: Bruce Schneier, "Secrets and Lies: Digital Security in a Networked World"

Rob Slade <rslade@sprint.ca>

*Mon, 30 Jul 2001 09:54:29 -0800*

BKSECLIE.RVW 20001022

"Secrets and Lies: Digital Security in a Networked World", Bruce Schneier, 2000, 0-471-25311-1, U\$29.99/C\$41.95

%A Bruce Schneier schneier@counterpane.com

%C 5353 Dundas Street West, 4th Floor, Etobicoke, ON M9B 6H8

%D 2000

%G 0-471-25311-1  
%I John Wiley & Sons, Inc.  
%O U\$29.99/C\$41.95 416-236-4433 fax: 416-236-4448  
pfurlong@wiley.com  
%P 412 p.  
%T "Secrets and Lies: Digital Security in a Networked World"

"Secrets and Lies" has generated a great deal of interest in the security community this year. Much of this interest probably stems from the simple fact that it isn't every day (or every year) that you get a general security book, written for the non-specialist, produced by a major name in the field. But one point seems to have been glossed over in the praise for this work. Schneier's writing is lively, entertaining, and even playful throughout the entire book. Not only is this volume a realistic and useful view of the security enterprise, but it's a lot of fun.

As the author of "Applied Cryptography," the leading text in the field; the founder of Counterpane Systems, with its major influence in encryption consulting; and the publisher of the Crypto-Gram newsletter, regular and thoughtful analyses of major encryption related issues; Bruce Schneier is, among the technically and cryptographically knowledgeable, arguably more influential than many academics whose names might be more widely known in relation to specific algorithms. So when Schneier states, in the preface, that cryptography is not "The Answer(TM)" to security, you have to take him seriously. He goes on, in the introductory chapter, to point out that "The Answer(TM)" does not exist: securing complex systems is a hard job purely

because the systems are complex, and any easy answer is bound to be wrong.

The price of digital reliability is constant vigilance. As such, don't come looking to this work for easy answers or cookbook solutions. What you will find is a solid introduction, and more, to the problems you have to overcome to keep your information safe, and some guidelines on how to go about the task.

Part one is an overview of the field of network operations with a view to restricting some ideal definition of "secure" to a more achievable goal.

Chapter two describes a number of digital threats (aside from the mention of salami attacks, quite realistically) and points out that none of the crimes are new, although the extreme of accessibility is. Various attacks, and various motivations, are reviewed in chapter three. The discussion of different types of adversaries, in chapter four, provides a reasonable assessment of the whole range from script kiddies to infowarriors, and compares relative levels of competency and risk tolerance. Chapter five outlines security needs and, again, points out that all computer security measures have their origins in physical security practices we all take for granted.

Part two looks at the various technology components of security and security systems. The writing in this section is a little more mundane and less sparkling than other parts of the book, but the material is reliable and convincing. Chapter six is, of course, an excellent primer on

the basic concepts and applications of cryptography. The analysis is extended to "real world" limitations and faults with encryption in chapter seven, including an intriguing comparison of proprietary protocols and alternative medicine. Chapter eight discusses computer security in broad terms, but concisely expresses concepts and models that many other books waste pages on without ever making the fundamentals clear. (It also provides some amazing, and occasionally amusing, glimpses into the lack of security in Microsoft's Windows.) Authentication is described well in chapter nine. Chapter ten is oddly unstructured. Entitled "Networked- Computer Security" it starts off with viruses and malware, talks a bit about operating system architecture, and ends up with some Web insecurities. While there are errors (particularly in the virus section) most of the material is not really bad: it just seems strange in comparison to the earlier chapters. Network Security, in chapter eleven, returns to the original level of focus, and explains various concepts using TCP/IP as an example. Chapter twelve takes a depressing, but accurate, look at the major network security tools, as well as making the important, though counterintuitive, point that false alarms can be worse than no security at all. Software reliability gets a fairly standard treatment in chapter thirteen, and much the same is true of hardware security in chapter fourteen. As might be expected, the coverage of certificates and the public key infrastructure, in chapter fifteen, clearly sets forth all necessary considerations and weak points

to examine.

Technical books usually have some catch-all chapters, but not all of them admit it up front. Chapter sixteen touches on a number of tricks that people have relied on to protect data, and uses devastating logic to point out why said stunts don't work. Finally, in chapter seventeen, we come to the largest source of security problems, and the one we can't do anything about: people.

The first two parts look at problems. Part three tries to present some solutions, or at least approaches to solutions. Chapter eighteen describes the vulnerability landscape, and suggests following the process of attacking a system, in order to identify how much security is needed at certain points, and weak areas that may need to be reinforced somehow. (This is a far cry from the "how to hack" tools lists of some of the more sensational "security" books, and much more useful.) Risk assessment, in chapter nineteen, is reasonable and balanced, but not great. Chapter twenty is disappointing, in that it is entitled "Security Policies and Countermeasures" but concentrates on a series of specific examples of good and bad security systems. Elsewhere the book promotes the fact that without a policy you have no security. It therefore seems a bit of an abdication of the topic to leave it without much discussion of the actual production of a policy. Attack trees might be seen as yet another example of a tool more useful to the security breaker than the sysadmin, but chapter twenty one's explanation shows how it can structure the task of analyzing

protective measures. This process is far more likely to succeed than a vague injunction to secure everything, and this chapter alone probably makes this work a "must have" for every security library. Product testing, in chapter twenty two, deals mostly with how \*not\* to evaluate software, and includes a good discussion of full disclosure and the open source movement. However, I can definitely sympathize with the position of the latter part of the chapter: potential security is pointless, what really counts is how secure a system is when set up by the typical harried administrator. The future is usually left for last, but Schneier takes a solid look at likely trends and paints an alarming, if not completely apocalyptic, picture. Chapter twenty four supports one of the major theses of the book: security is a process, not a product. Therefore, the chapter provides a set of guidelines, attitudes, points, and general principles to be used in looking at security as a process. The conclusion, in chapter twenty five, seems to be that lots of people are trying to avoid their proper responsibility for security, but the task is achievable.

Quite apart from the general readability of the text, Schneier has ensured that the content and explanations are accessible to any intelligent reader. You do not need specialist training to understand the concepts presented herein. And the concepts encompass pretty much everything to consider about security in a networked world. This is one of the very few books that I

feel I can recommend without reservation to a newcomer concerned about computer or communications security. It presents the situation clearly, with real explanations of the dangers, but no overpromoted sensationalism.

If the volume seems a bit long all I can say, with Schneier, is that security is complex. The book has very little wasted space.

I can also say that security professionals will not regret time spent with it. We tend to need more frequent reminding than teaching, and the comprehensive coverage touches on many issues that are important, but may be ignored as not always being urgent. However, the book also does an excellent job of explaining some specialty and esoteric topics. Hopefully "Secrets and Lies" will have a prominent position on many security library shelves.

copyright Robert M. Slade, 2000 BKSECLIE.RVW 20001022  
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 21: Issue 56**

**Thursday 2 August 2001**

## Contents

- [NASA data from 1970s lost due to "forgotten" file format](#)  
[Aaron Dickey](#)
- [Motorola Stock Drops 99.95%!](#)  
[Daniel Norton](#)
- [JDS Uniphase quarterly results hacked? NO!](#)  
[Dave Isaacs](#)
- [Freeware app to retrieve passwords from Internet Explorer](#)  
[Lyle H. Gray](#)
- [Totally Hip with spyware](#)  
[Michael F. Maggard](#)
- [Medical records via e-mail](#)  
[William Colburn](#)
- [AS IF: draft-ietf-dnsext-ad-is-secure-03.txt](#)  
[John Gilmore](#)
- [Microsoft's PGP keys don't verify](#)  
[Brian McWilliams](#)
- [Telling all to the police](#)  
[Norm deCarteret](#)
- [Identity theft](#)  
[Jack Holleran](#)

- [Risks of profanity filtering](#)  
[Paul Bissex](#)
  - [Car-door lock remote control activates another car's alarm](#)  
[Mark Brader](#)
  - [S-not-SL](#)  
[Mike Albaugh](#)
  - [Re: MSN security upgrade forces new e-mail address](#)  
[Robert J. Woodhead](#)
  - [No Appleplexy needed](#)  
[Dave Stringer-Calvert](#)
  - [Re: Autoresponder goes haywire](#)  
[Richard Johnson](#)
  - [Re: Erroneous air navigation reading](#)  
[Mike James](#)
  - [Re: Polarized sunglasses and LCD frustration](#)  
[Chris J Dixon](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

## ⚡ **NASA data from 1970s lost due to "forgotten" file format**

Aaron Dickey <wnnaaron@yahoo.com>  
*Sat, 28 Jul 2001 23:31:43 -0700 (PDT)*

In 1999, USC neurobiologist Joseph Miller asked NASA to check some old data the Viking probes had sent back from Mars in the mid-1970s. Miller wanted to find out whether certain information on gas released by Martian soil, which at the time had been dismissed as meaningless "chemical activity," was actually evidence of microbial life. NASA found the tapes he requested, but they didn't find any way to read them. It turns out that the data, despite being only about 25 years old, was in a format NASA had long

since forgotten  
about. Or, as Miller puts it, "The programmers who knew it had  
died."

Luckily, Miller has been able to cobble together about a third  
of the data  
and get some useful results, but only because some form of  
printed record  
had been saved. (And yes, he does believe the Viking probes  
turned up  
evidence of microbes.)

Source: Reuters. Original article is available, at least  
temporarily, at  
<[http://dailynews.yahoo.com/h/nm/20010727/sc/  
space\\_mars\\_life\\_dc\\_1.html](http://dailynews.yahoo.com/h/nm/20010727/sc/space_mars_life_dc_1.html)>,  
<[http://news.excite.com/news/r/010727/19/science-space-mars-life-  
dc](http://news.excite.com/news/r/010727/19/science-space-mars-life-dc)>,  
<<http://reuters.activebuddy.com/s?id=DS1DEKNG8BBN>>, or  
<[http://www.reuters.com/news\\_article.jhtml?type=sciencenews&  
StoryID=137333](http://www.reuters.com/news_article.jhtml?type=sciencenews&StoryID=137333)>.

---

## 🚩 Motorola Stock Drops 99.95%!

Daniel Norton <[danorton@suespammers.org](mailto:danorton@suespammers.org)>

*Thu, 02 Aug 2001 10:17:06 -0400*

My Yahoo! alerts window popped up with an explosive sound this  
morning to  
notify me that Motorola's stock (MOT NYSE) value crashed.  
Incredulous, I  
went to the Yahoo! Finance page and confirmed it. Undaunted, I  
proceeded to  
the NY Times finance site which only concurred. Finally the  
NYSE site  
confirmed that, in fact, the value of MOT had been exactly one  
penny  
(US\$0.01) at the open, but rebounded spectacularly, even to

exceed the  
previous day's close! (cf. <http://www.danielnorton.net/mot.gif> )

Hopefully, anyone who automates trading programs around this kind of glitch (It was a glitch, wasn't it?), but we RISKS readers know that such hopes aren't always fulfilled.

Daniel Norton

---

## **🔥 JDS Uniphase quarterly results hacked? NO!**

Dave Isaacs <dave.isaacs@entrust.com>

*Mon, 30 Jul 2001 09:39:49 -0400*

I saw this interesting aside in an *\*Ottawa Citizen\** article (27 Jul 2001)

about JDS Uniphase's latest quarterly results:

"The world's largest maker of fibre optic components was forced to halt the trading of its stock for most of the afternoon yesterday because a hacker broke into its corporate network and stole a draft copy of the company's fourth-quarter results. It had been released before the markets closed yesterday afternoon."

The article is at

<http://www.ottawacitizen.com/business/010727/5066222.html>

The obvious risk here is the consequences of storing very valuable information unencrypted on a network-accessible computer. Nothing new in

that lesson. What would be interesting is knowing is \*how\* JDS Uniphase knew that this break-in had occurred, and what form the break-in took. It sounded like a story we'd all be interested in hearing.

A further article, from the \*Globe & Mail\* (28 Jul 2001), with the rather convoluted URL of

[http://rtnews.globetechnology.com/servlet/RTGAMArticleHTMLTemplate/C,C/20010](http://rtnews.globetechnology.com/servlet/RTGAMArticleHTMLTemplate/C,C/20010728/wfhack?tf=RT/fullstory_Tech.html&cf=globetechnology/tech-config-neutral&slug=wfhack&date=20010728&archive=RTGAM&site=Technology)

[728/wfhack?tf=RT/fullstory\\_Tech.html&cf=globetechnology/tech-config-neutral&](http://rtnews.globetechnology.com/servlet/RTGAMArticleHTMLTemplate/C,C/20010728/wfhack?tf=RT/fullstory_Tech.html&cf=globetechnology/tech-config-neutral&slug=wfhack&date=20010728&archive=RTGAM&site=Technology)

[slug=wfhack&date=20010728&archive=RTGAM&site=Technology](http://rtnews.globetechnology.com/servlet/RTGAMArticleHTMLTemplate/C,C/20010728/wfhack?tf=RT/fullstory_Tech.html&cf=globetechnology/tech-config-neutral&slug=wfhack&date=20010728&archive=RTGAM&site=Technology) contains more details. Apparently, there was no 'hacker' or 'break-in'.

JDS had placed the release on their Web site. A sharp-eyed surfer noticed that if you type in the exact file name, up pop the results. I suspect that a document-naming convention was apparent from looking at previous financial results.

As to how JSU found out about the 'break-in': the 'hacker' phoned them up and told them.

Dave Isaacs <dave.isaacs@ottawa.com>

[JDS apparently reported a \$51 billion loss for the year ending 30 Jun 2001, and 16,000 jobs lost. PGN]

---

## **🔥 Freeware app to retrieve passwords from Internet Explorer**

"Lyle H. Gray" <gray@cs.umass.edu>  
*Mon, 23 Jul 2001 22:24:15 -0400 (EDT)*

The following item appeared in the "Download This" section of the Earthlink Weekly Email Newsletter on 07/23/2001:

\* Windows: Password Recovery

[http://www.iopus.com/password\\_recovery.htm](http://www.iopus.com/password_recovery.htm)

If you tell your browser to save Web site passwords so that you don't have to reenter them, you might forget those passwords over time. This program can reveal the passwords hidden behind those asterisks in Web site login screens. (Freeware)

This item highlights an inherent risk of allowing IE to save your passwords (other than the obvious one that anyone with physical access to your system would also have access to your password-protected pages): Someone with access to your system may be able to determine a pattern to your password choices (especially if you only have one password...)

[and also to use your IE passwords directly while masquerading... PGN]

---

## **✶ Totally hip with spyware**

"Michael F. Maggard" <mbear@bigfoot.com>

*Tue, 31 Jul 2001 17:32:24 -0400*

Recently it was discovered that the Mac software "Livestage Pro" by Totally Hip software has been reporting back its license, usage, and environment to its manufacturer via a covert http dialogue.

The company has refused to respond to the discovery "officially", but one of their staff members has been corresponding publicly on the

popular Mac  
website at <http://www.macintouch.com/spyware.html>. There he's  
expressed  
surprise that anyone is concerned and asserts his business has  
the full  
right to include this sort of tracking, that it is noted deep in  
one of the  
readme files and permission to "electronically verify their  
serial number "  
is specified within the software license.

The non-representative goes on to state that in the future  
Totally Hip  
intends to somehow secure the collected information and this is  
all simply a  
legitimate anti-piracy effort. Finally he's taken the Web site  
to task for  
posting letters that detail how to block the reporting function  
(edit one's  
hosts file), likens it to supporting software piracy and closes  
with  
"Honestly we are not an evil conspiring company."

This isn't an isolated incident for Mac software developers;  
powerhouse  
Adobe has been installing a mysterious file of their own that  
regularly  
"calls home" for reasons unknown. Adobe has promised to explain  
this new  
feature, what it does and what it is communicating but to date  
have not  
followed through.

---

## **✶ Medical records via e-mail**

"Schlake ( William Colburn )" <schlake@nmt.edu>  
*Mon, 30 Jul 2001 15:31:52 -0600*

I live in a small town. Two of the doctors I visit have been my doctors my entire life, and the third in the office has been a friend of the family just as long. The office has been run virtually the same my entire life (they still have the original monochrome monitors on their office PCs). The newest doctor, however, demanded some new-fangled ideas as part of her contract to work there. She makes recordings of her medical notes and they are transcribed by a third party company. The transcriptions come via e-mail (which the office can't receive) in MS word 2000 (which the office can't read), so she gets them at her house and prints them out. She is out of town for three weeks now, and they asked me to take care of this for them. I don't know if my experience is typical of the medical transcription business, but I suspect that it is.

The transcriptions are made at the office from the doctor reading her notes onto tape. I didn't ask, but I suspect that the tape is then mailed or shipped to the transcription agency. The employee there then types up the information and e-mails it back out to the "appropriate place". The e-mail is not (cryptographically) signed, nor is it encrypted. In the case of my local office, it goes from the ISP of the person doing the work to a local ISP here in Socorro. The doctor has a wireless link from her house to the ISP and uses an unencrypted POP session. The transcripts are then launched from outlook into word, and printed out. She saves a local copy onto her hard disk (just in case) and deletes them from the server.

These documents can contain a lot of information. A medical history will include tremendous personal data on not just the patient, but on their entire family, including date of birth and lifestyle. A simple office visit can be mundanely bland (a broken wrist) to life-shatteringly personal (someone here was inspired by "Bobbitt"), but always contains the persons real name, complaint, diagnoses, and prescription.

There are numerous places along the trip that this information could fall into the wrong hands. A virus could be present at either end of the e-mail which might compromise data. The data passes through ISPs in the clear, and could be intercepted or modified while in transit. The wireless ISP is like a scrolling marquee if someone has the right equipment. Outlook likes to "keep e-mail on the server" even if the user has deleted it, so all those transcripts could still be on the local ISP. And lastly, a copy of everything is stored on her computer in her house and not in the security of the office.

I often tell people that I have "no delusions of privacy" in our modern world. It keeps me sane.

---

## **AS IF: draft-ietf-dnsext-ad-is-secure-03.txt**

John Gilmore <gnu@toad.com>  
*Sat, 28 Jul 2001 12:16:53 -0700*

I think some of you guys have gotten so tied up in micromanaging DNS

Security implementation details that you forgot what swamp we were trying to drain.

There is no point in building a cryptographically-secured DNS in which many of the machines will be configured to "just believe whatever they are told, regardless of the cryptographic signatures"!

We already have such a DNS -- today's. It doesn't need signatures or AD bits or big packets or any other changes. Anyone who is happy with that can go home and stop arguing. The rest of us are interested in the real security and integrity of the Internet.

Any client implementation that listens to a single bit of the response to tell it whether the response is cryptographically valid must be considered noncompliant with the DNSSEC spec. It's just an old fashioned insecure DNS client. There's nothing wrong with that, as long as you don't have any high trust expectations for it.

Any server which deposits a single bit in the response to claim to clients that it has cryptographically validated the results, so they don't have to, is just encouraging the above abuse.

I'm not shocked to find people advocating that such a server actually lie to the clients about whether it has validated the data. The entire model (trusting a packet to tell you whether somebody else has validated the data) provides ample opportunities for not only your

friends but your enemies to lie to you. Just like in the current DNS.

John

PS: I know, I know, the "valid" bit will be secured by some "out of band" means. Like a shared static key, and/or by the security of the file system on the server. Right. For extra credit: composing several weak security primitives produces what? Strong security or weak security?

PPS: The real question is why anyone is advocating that the DNS be "secured" by lame security. There are challenges aplenty even when you're working with strong primitives; trying to mix in weak stuff is just wasting everyone's time. People have encouraged me in the past to assume the possibility of mere incompetence rather than assuming actual malice (e.g. when the FBI's Louis Freeh testified to Congress about the security of DES). So: Were any of you on the standards committees for cellphone privacy? How about on the 802.11 "Wiretap Equivalent Privacy" committee? Did any of you have a hand in shortening the key in DES? Perhaps you designed the encryption scheme used in DVDs or in Adobe eBooks? Whether you're incompetent or malicious, stick to breaking codes, it's much easier. Especially when you break them in the standards committee before they're deployed.

---

**Microsoft's PGP keys don't verify**

Brian McWilliams <brian@pc-radio.com>

Thu, 26 Jul 2001 15:33:10 -0400

[From Dave Farber's IP, archived at  
<http://www.interesting-people.org/>

Submitted by Ben Laurie, who commented that

As the immortal phrase has it, "the RISKS are obvious."  
PGN]

FYI ...

Microsoft Bulletins Fail PGP Verification

<http://www.newsbytes.com/news/01/168397.html>

For at least four months, Microsoft has been sending out security bulletins which fail a popular e-mail authentication system. As a result, the company could be opening the door to counterfeit bulletins from malicious hackers.

To protect against forgery, Microsoft's security response center digitally signs its bulletins with PGP before e-mailing them to subscribers of its security notification service. But since at least March, if recipients attempt to verify the messages' authenticity, PGP will issue a warning that the bulletins contain an invalid signature.

"The problem is that Microsoft's bulletins effectively look as if they're forged. And telling a Microsoft forgery from someone else's is virtually impossible," said Paul Murphy, head of information technology at Gemini Genomics, a genetic research firm in Cambridge, England. [...]

## **⚡ Telling all to the police**

Norm <nsdec@mercurylink.net>

*Fri, 27 Jul 2001 18:06:01 -0400*

\*The New York Times\* reports (27 Jul 2001) on 17 Jul theft from 9 lockers at an upper East Side sports club. Directly after they called the police a call was received from "the police fraud department" and 4 victims responded to a series of questions and gave their credit card numbers, husbands names, SSN, PINs and mothers' maiden names. Anything wrong with that? That is, aside from when the police did arrived they said there is no such dept.

One womans tale: she called the credit card issuers but couldn't reach her bank, being after hours and all. The next morning she found \$500 had been taken using her bank card.

The Risk, stupidity or cupidity aside, is being unlucky enough to be a victim outside bankers hours ... and in a bank not having a 24-hour notification phone#. There Oughta Be A Law, as credit cards, that limits consumer loss to \$50 for such cases.

(PS: the same woman said she had worked out daily until then but "Now I am so paranoid I haven't been back". That's probably the wrong lesson learned).

Norm deCarteret      NSDEC Inc

## ✶ Identity theft

Jack Holleran <Holleran@severnapark.com>

*Fri, 27 Jul 2001 00:12:26 -0400*

It would interesting to see what the vetting process was for the salesperson(s)? There seems to be an incredible amount of information that was revealed without (m)any controls in place.

Huge identity theft uncovered; Files with Social Security and driver's

license numbers pasted in chat room; possible link to cell phone

applications, By Bob Sullivan, MSNBC, 25 Jul 2001

Key personal data belonging to hundreds of individuals have been shared in

an Internet chat room, in what one expert says could become one of the

largest identity-theft cases ever. The data include Social Security

numbers, driver's license numbers, date of birth and credit card

information - everything a criminal would need to open an online bank

account, apply for a credit card, even create the paperwork necessary to

smuggle illegal immigrants. It is still unclear how the data ended up in

the chat room, but an MSNBC.com investigation has revealed common threads

among the victims - including the purchase of a cell phone online from

VerizonWireless.com or an AT&T Wireless reseller.

Full text of the article can be found at

<http://msnbc.com/news/604496.asp?cp1=1>

## ⚡ Risks of profanity filtering

Paul Bissex <pb@e-scribe.com>

*Thu, 19 Jul 2001 20:36:19 -0400*

Observant readers will have already noted that my last name contains the word "sex." Recently, in trying to register with a Web site -- using my real name -- I was chastised for "profanity" and asked to choose a different ID.

I declined, and since the company has offered no response to my inquiry as to whether this policy is really necessary, I thought I'd share the screen grab:

<http://bissex.net/paul/profanity.gif>

The business risk, alienating customers, is fairly obvious. More broadly, this highlights a familiar problem with "bad-word list" censorware. Imagine if this were an e-mail filter on a firewall instead of a registration script.

Paul Bissex, CEO, e-scribe.com

---

## ⚡ Car-door lock remote control activates another car's alarm

Mark Brader <msb@vex.net>

*Tue, 31 Jul 2001 17:51:01 -0400 (EDT)*

[The following was posted by "K.D." <kayemmdee@hotmail.com> in alt.fan.cecil-adams; forwarded to Risks by Mark Brader with the author's permission.]

On at least three occasions, my battery-operated car unlock remote control set off the car alarms in nearby vehicles. I found that I could turn on the alarm, and with another press of the remote control, turn it off. Ad infinitum.

The most astounding of these was the first time it happened (in Rochester, NY). But not simply because this was new information that I could set off the car alarm. Rather, because of the reaction of the owner of the other car.

At first, I didn't realize how it was that the nearby car alarm had been triggered, since neither we or anyone else was close to the vehicle. Eventually, I figured out that \*I\* had done it with my remote control. I also figured out that I could turn the alarm off as well as turn it on.

As we continued to approach my car, it also dawned on me that the owner of the vehicle in question was also coming across the lot. I pointed to the previously alarm-sounding vehicle, and asked if it was his. He said that it was. Lest he had observed what had just occurred and somehow thought I was up to no good, I said, "It seems that my remote control activates your car alarm." His response? "I don't have a car alarm." I looked at my sister, who was as perplexed as I was, and decided not to argue / explain.

Perhaps I should mention that there was no other vehicle nearby that could have been sounding the alarm. It was not my vehicle. Especially now that it has happened two other times, I am sure my remote control triggered his alarm.

One bummer about this is thus: You open your car door. The other person's alarm goes off. You press the remote control again to shut off the alarm and naturally your car door locks again. So, you have to unlock your car door, the alarm of the other car goes off, you open your car door so you can get in your car, and then you press the remote control again to shut off the other car alarm.

I suppose if you just gave the alarm enough time, it would shut off on its own.

[K.D. then posted this followup]

In re-reading my post, I realized that this is screwed up. Yes, when you hit the remote control again ("unlock"), the door lock makes a sound. However, I now realize that it isn't re-locking -- just making that unlocking sound again.

I think. At the time (second incident), I recall that when I tried to get into my car after turning off the other person's car alarm, I found that my door was locked. Duh -- I had just unlocked it. I then assumed that I had relocked my car door, even though I had presumably used "unlock" to turn off

the alarm, as that is the button I had used that resulted in the alarm turning on.

Damn -- if and when this happens again (so far, three times in about as many months), I'll have to study the phenomenon more closely.

-KD

---

## ✂ **S-not-SL (Re: SSL, [RISKS-21.53,54](#))**

Mike Albaugh <albaugh@spies.com>  
*Mon, 23 Jul 2001 16:07:25 -0700 (PDT)*

I have found the following analogy useful, explaining to laypersons the "Security policy" most common on the Web:

"Imagine a restaurant that assigns armed guards to escort your credit-card to the cash-register and back, then tacks all the carbons to the employee-bulletin-board, right inside an un-locked back door"

Most of them get it immediately.

---

## ✂ **Re: MSN security upgrade forces new e-mail address (Silberman, [R-21.54](#))**

"Robert J. Woodhead (AnimEigo)" <trebor@animeigo.com>  
*Mon, 23 Jul 2001 19:52:39 -0400*

"Ami A. Silberman" <silber@mitre.org> wrote:

>The risk? MSN's attempt to improve security (apparently by forcing spammers  
>to modify their software to change fake msn addresses) has resulted in  
>additional burden on list administrators.

You think that's bad? I've been maintaining a bounce-management tool for a mac-based listserv app, and as such, I see a lot of weird bounce formats, many of which make the extraction of the bouncing e-mail address quite a challenge.

But the all-time champ is a certain large ISP who shall remain nameless but whose initials are a, o & l. If one of their users has redirected his e-mail to another ISP, and the final destination e-mail address bounces, then our friendly large ISP sends a polite bounce message back that clearly contains the final destination e-mail address.

Alas, since it doesn't contain the original destination e-mail address, it is impossible to determine who to unsubscribe; forevermore, you have a "zombie" in your mailing list.

The listserv, alas, doesn't attach a useful header like "Original-Recipient:" that could be used to identify the zombie because it tries to conserve bandwidth by grouping e-mails to the same domain name into a single transaction.

If mail servers added an "Original-Recipient:" header if they have to forward the e-mail (and there isn't already one in the headers), life would be immeasurably easier for bounce management. A standard for

bounce

reporting that made life easy for nonhumans would also seem to be an obvious idea.

Needless to say, an e-mail to the large ISP mentioning the issue seems to have gotten sucked into a black hole.

Robert Woodhead, CEO, AnimeEigo <http://www.animeigo.com/>  
<http://selfpromotion.com/> The Net's only URL registration  
SHARESERVICE.

---

## **⚡ No Appleplexy needed (Re: [RISKS-21.55](#))**

Dave Stringer-Calvert <dave\_sc@csl.sri.com>  
*Tue, 31 Jul 2001 16:13:52 -0700*

The Apple-DNS-hacked item in the latest risks is not a hack - it's a "legitimate" use of the NIC records. Someone has registered hosts with the NIC who just happen to have apple.com in their name. The same thing has been done to Microsoft:

```
; whois microsoft.com@whois.internic.net  
[whois.internic.net]
```

```
MICROSOFT.COM.Z---HELLO-FROM-SIBERIA---I.Z3S.COM  
MICROSOFT.COM.WILL.NEVER.SATISFY.A.TRUE.TELNETJUNKIE.COM  
[... and so on into the night]
```

[This was noted by MANY readers. TNX. Sorry for my immoderate lapse.  
PGN]

## ✉ **Re: Autoresponder goes haywire (Bieber, [RISKS-21.51](#))**

<rjohnson@ucar.edu>

Sun, 22 Jul 2001 11:21:43 -0600 (MDT)

In [RISKS-21.51](#), Joshua M Bieber mentioned the following problems that led to a quite typical autoresponder flood of one of his mailing lists. In addition to the suggested protective measures, it may also be wise for the list to send with the original sender's address as the From/Reply address, instead of using the list broadcast address there. That way, only one person gets nailed with the inappropriate autoresponse. That's still unacceptable behavior, but at least the damage is less severe that way.

Better yet, however, is deleting that bogus autoresponder software. Any autoresponder that replies to a message where:

- 1) the Precedence header indicates Bulk or List, or where
- 2) the user's address does -not- appear in the To or Cc header

is broken software. The author of such an autoresponder should at least be hauled out behind the barn for a strapping.

The problem illustrated by Guilty Person, in cahoots with the author of the broken autoresponder used, is that of continually rewriting the same piece of software with the same old mistakes. In this case, it's particularly ludicrous; properly operating examples of 'vacation' have been

available  
for free for 20 years.

Richard Johnson

---

**✂ Re: Erroneous air navigation reading (Hopkins, [RISKS-21.53](#))**

Mike James <mike@hamble.demon.co.uk>

*Mon, 23 Jul 2001 21:54:24 +0100*

That description of an aircraft navigation system out by 14 degrees on a bearing posted by Bill Hopkins reminds me of a 'trick' I played on myself.

Take one Garmin GPS 12(XL), 38, 45, 48 .... Probably most handheld GPS units.

Set user compass variation...

setup->navigation->heading->user and enter 180 degrees

Now navigate to a waypoint. The bearing to waypoint will be displayed as asked, but 180 degrees out. The 'compass' display arrow correctly contradicts the bearing given.

This is confusing but totally correct. Just be careful....

Smaller numbers would be less obvious as in the aircraft case.

I was only yacht racing in the Solent and the error was obvious. Crashing off a mountain by using a magnetic compass and a GPS misconfigured like this could be worse. (standing still need magnetic compass for current heading)

---

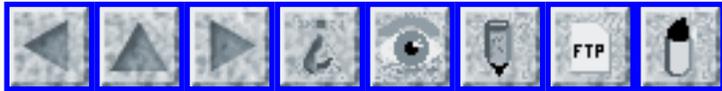
**⚡ Re: Polarized sunglasses and LCD frustration (Boyd, [RISKS-21.54](#))**

Chris J Dixon <chris.dixon@easynet.co.uk>

*Fri, 27 Jul 2001 19:06:45 +0100*

Surely it is the other way round. Displays are not fussy about the polarisation angle, but sunglasses are specifically oriented so that they are most effective at intercepting light reflected off (and polarised by) horizontal surfaces.

Chris J Dixon Nottingham UK <chris.dixon@easynet.co.uk>



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 21: Issue 57**

**Tuesday 7 August 2001**

## Contents

- [WEP insecurity](#)  
[Avi Rubin](#)
- [European Union strives for openness](#)  
[Stephen A. Boyd](#)
- [WinXP blocks some versions of some programs](#)  
[B. Elijah Griffin](#)
- [Cyanide for Code Red](#)  
[Jeremy](#)
- [I am virus generator?](#)  
[Bob Frankston](#)
- [AT&T Worldnet exposes all user passwords](#)  
[Una Smith](#)
- [Password changes -- SIGH!](#)  
[Jim Horning](#)
- [The risks of online order tracking](#)  
[Darryl Smith](#)
- [Mixing advertising and credit-card activation](#)  
[Bob Green](#)
- [Techs must report child pornography](#)  
[Brien Webb](#)

- [Re: Dutch government and virtual child pornography](#)  
[Christian Reiser](#)
  - [Re: Super-accurate atomic clock hates Sundays](#)  
[Phil Kos](#)
  - [What is your area code, really?](#)  
[Andrew Koenig](#)
  - [Online advertising: Fraud, false positives and a novel DOS attack](#)  
[John O'Connor](#)
  - [Re: Even a fatal error can't kill it](#)  
[Terry Brugger](#)  
[Joe Thompson](#)  
[John M. Hayes](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

## ⚡ WEP insecurity

Avi Rubin <rubin@research.att.com>

*Tue, 07 Aug 2001 05:56:27 -0400*

[Read it and WE(E)P, unless you already WEpt. PGN]

We have a new paper:

Using the Fluhrer, Mantin, and Shamir Attack to Break WEP  
by

Adam Stubblefield, John Ioannidis, and Aviel D. Rubin

We implemented an attack against WEP, the link-layer security protocol for 802.11 networks. The attack was described in a recent paper by Fluhrer, Mantin, and Shamir. With our implementation, and permission of the network administrator, we were able to recover the 128-bit secret key used in a production network, with a passive attack. The WEP standard uses RC4 IVs

improperly, and the attack exploits this design failure. This paper describes the attack, how we implemented it, and some optimizations to make the attack more efficient. We conclude that 802.11 WEP is totally insecure, and we provide some recommendations.

The paper is available at <http://www.cs.rice.edu/~astubble/wep/>

Avi Rubin, AT&T Labs - Research <http://avirubin.com/>

White-Hat Security Arsenal: <http://white-hat.org/>

---

## ✶ European Union strives for openness

"Stephen A. Boyd" <UncleHonus@aol.com>

*Fri, 3 Aug 2001 13:01:18 EDT*

The European Commission issued a White Paper last week that aims to address widespread public dissatisfaction with politics by increasing the openness and accountability of European Union institutions.

"Many Europeans feel alienated from the Union's work," according to the White Paper, and they "no longer trust the complex system to deliver what they want."

The White Paper identifies five principles that define "good governance"

Openness, Participation, Accountability, Effectiveness, and Coherence.

The Paper goes on to identify proposed changes in European Union policy derived from these principles.

"We simply cannot go on as we are," said European Commission President

Romano Prodi. "The White Paper is not an instant cure for everything, but

it is a serious attempt to address the concerns that many people have."

To a American reader, the White Paper's diagnosis of public disenchantment

with politics is familiar. Its prescription, however, may seem a little

naive in its faith that political life can be reinvigorated through

procedural changes. Even so, it is a refreshing reminder that political

institutions are not simply inherited, but are also maintained and can be

recreated by regular people.

"European Governance -- A White Paper" was adopted by the European

Commission on July 25 and published for public comment here:

[http://europa.eu.int/comm/governance/white\\_paper/index\\_en.htm](http://europa.eu.int/comm/governance/white_paper/index_en.htm)

First, the source: This commentary was copied and pasted directly from

\*Secrecy News\*, a digest (but not a forum) written by Steve Aftergood, an

employee of the Federation of American Scientists (<http://www.fas.org>).

Second, the irony: It is ironic that, on one hand, the EU ministers would

issue statements like this, while on the other hand, they are pursuing the

ECHELON continental-wide wireless surveillance and monitoring network. I

guess "openness", the ministers contend, must go both ways, regardless of

any privacy issues the EU's constituency may have.

Third, the RISK: I believe this veil of purported openness is a valid RISK,

since it seems the EU chiefs are making a push for pulling the wool over their constituents eyes. The issue Mr. Aftergood astutely mentions of "public disenchantment" is not only reinforced, it seems, but gives Americans no more confidence in our own government with respect to privacy and auto-accountability issues, since the same game is being played here. I'm all for good government and a solid nation, but only when the members of those governments are accountable to their bosses (i.e., the People).

Stephen

---

## ✶ WinXP blocks some versions of some programs

"B. Elijah Griffin" <eli@panix.com>  
*Thu, 2 Aug 2001 16:33:13 -0400 (EDT)*

\*The Register\* reports that WinXP 'Release Candidate 2' has a driver block that will prevent a number of programs from running. Some people are apparently worried that MS might become too bossy about what software their OS can run.

The full story:  
<http://www.theregister.co.uk/content/4/20805.html>

Elijah

---

## **✶ Cyanide for Code Red**

"Jeremy" <jeremy@electrosilk.net>

*Mon, 6 Aug 2001 10:55:07 +0800*

Code Red may or may not be the major disaster that CERT predicted. It is certainly present and apparently mutating already.

What does not seem to have happened is the production of an effective stopper for the Code Red. Present prophylactic activities involve getting as many systems as possible updated with 'the fix'. This of course will not work as a large number of systems are run out of the box by people with little to no technical training. They won't even know how to recognise they have the worm, let alone fix it.

One simple fix is a passive worm that sits on a target machine and when a Code Red attack arrives, infects the attacker using the same technique that Code-Red uses (by definition, an attacking machine must be vulnerable to the attack). The passive worm could disinfect the attacker, and then sit waiting for further attacks on the original machine plus on the newly disinfecting attacker. The rate of spread of the passive worm would be directly proportional to the spread of Code-Red. The passive worm cannot spread at all unless Code-Red is operating.

The passive worm would almost certainly disable the IIS service, in fact it might be a good idea to have it produce a default web page stating so, together with instructions on how to download the security fix.

An improved version may even apply the fix itself.

The question arises as to whether a passive worm is illegal in any way.

The arguments for a passive worm are that the system it is defending is under attack and it is taking steps to stop that attack. As a by-product, the attacker is unable to attack any other systems. The attacker does not suffer any damage as a result of the disinfection.

The argument against it is that the defender places and executes code on the hostile machine. This may well breach any number of anti-virus laws.

The real test of the argument will be when a very dangerous worm, say like Code-Red but 100 times as potent, is unleashed. The various Governments will be left in the serious dilemma as to whether to allow a vital national resource be destroyed, or to unleash a probably illegal antidote.

The time scale to make such a decision could be a matter of hours from first discovery to Internet meltdown. Governments (and Microsoft) must have a contingency plan in place. I wonder what it is?

Jeremy

---

## **⚡ I am virus generator?**

"Bob Frankston" <RMFx18@Bobf.Frankston.com>

*Fri, 3 Aug 2001 14:50:28 -0400*

Norton Anti-Virus 2001 has decided that the script I use to backup my files is a virus. It says "Unable to repair this file OK" (no option for "Not OK")! In trying NAV2002 (beta) I found that it seems to label all scripts as viruses but, at least, it gives me an option of enabling them one by one by one. The trend to treat programming as a criminal act and put the onus on me to prove each action is not a crime is very worrisome. Outlook has the same attitude towards attachments, even URLs. It doesn't even deign to let me decide -- it just hides them.

I guess it goes along with viewing PEDs as terrorist devices. (For those who haven't been following the issue in RISKS -- Personal Electronic Devices seem to be viewed as too dangerous to allow on airplanes, at least during safety-critical portions of a flight such as taxiing to the terminal.)

Bob Frankston <http://www.Frankston.com> <<http://www.frankston.com/>>

---

## **✶ AT&T Worldnet exposes all user passwords**

Una Smith <una@lanl.gov>  
*Fri, 3 Aug 2001 17:27:59 -0600*

I called AT&T Worldnet customer support to ask a question about my bill. My question was entirely impersonal but nonetheless I was required to identify myself. I gave my name and current telephone number. The

service rep then asked me for the number I had when I signed up; when I hesitated, she volunteered it. Then she asked for my e-mail password. When I refused she informed me my password is not a secret, and that \*all passwords\* connected to my Worldnet account (a Worldnet account can have up to 6 e-mail accounts) are \*visible\* on her screen.

Una Smith, Los Alamos National Laboratory MS K-710, Los Alamos, NM 87545

---

## **⚡ Password changes -- SIGH!**

Jim Horning <horning@intertrust.com>

*Fri, 3 Aug 2001 12:12:52 -0700*

> From: <HR Department>  
> Sent: Friday, August 03, 2001 10:12 AM  
> To: <US Employees>  
> Subject: IMPORTANT <HR Database> INFORMATION - PLEASE READ  
>  
> We want to make you aware that <HR Database> will be unavailable from 6pm  
> (PT) on Friday, August 3 to 11:59pm (PT) on Sunday, August 5 due to server  
> upgrades. During this time, you will not be able to access the website.  
> In <Outsourced supplier>'s ongoing effort to improve site performance,  
> these upgrades are occurring to load balance and increase site stability.  
> Part of this site upgrade includes a password change. ALL USERS WILL HAVE  
> A PASSWORD OF "changel23" as of 12:01am PT Monday, August 6th, 2001. Once  
> you enter the system for the first time on or after August

6th, you will  
> be required to change your password and answer a secret  
question. In the  
> future, you will be able to use the answer to the question to  
reset your  
> own password.  
> If you experience problems, please contact the whereiwork help  
desk at  
> support@<Outsourced supplier>.

---

## ✶ The risks of online order tracking

"Darryl Smith" <darryl@radio-active.net.au>

*Mon, 30 Jul 2001 17:51:49 +1000*

I have just purchased a computer from Dell Computer. My  
experiences are  
interesting.

1. When I entered the 'E Code' to select the right configuration  
and price,  
the price given did not include the \$500 discount that I should  
have  
received. I ordered by phone and got the substantial discount.

RISK: Paying \$500 more on line.

2. Knowing that I might have problems with my credit (debit  
card) I  
specifically asked the credit union what my limit was per day.  
They told me  
that it was whatever my balance was. When I went to purchase  
this computer  
the purchase was declined. When I contacted the credit union by  
phone they  
informed me about a \$1000 per day limit unless it is up-ed but  
ONLY for the  
period that it was needed. I was to ring back as soon as the

transaction was completed.

RISK: Not having access to my money.

3. When I contacted DELL to let them know that the transaction could go ahead I was told that it would be a while for the transaction to occur - in other words they could not immediately process the transaction but it would be hours.

RISK: There was increased potential for fraud because my account limit was upped for longer than I would have liked.

4. Sydney is 10 hours ahead of GMT at the moment, meaning that most parts of the world are behind us. When I logged onto the tracking WWW site at 7AM I was told that what the status was at 8PM that day, or 13 hours ahead. But that night I checked it at 5PM and was told that the status was at 4AM that day, or 11 hours behind.

This does not make sense, unless the time is 11 hours behind at all times, and that the WWW site is reporting the clients day and the server time.

RISK: Times and Dates should be based on either the clients date and time, or the servers, but not a combination of the two.

5. The tracking WWW site notes that computer is in 'Delivery Prep' and has been for about 5 days and about to be shipped. When I checked up with DELL the computer had been shipped to Australia, and was at the Sydney warehouse for final delivery.

RISK: When relying on online order status systems, work out what the results mean before relying on them

Darryl Smith, VK2TDS POBox 169 Ingleburn NSW 2565 Australia  
Mobile Number 0412 929 634 [+61 4 12 929 634 International]

---

## ✶ Mixing advertising and credit-card activation

Bob Green <rgreen@etnus.com>  
*Mon, 30 Jul 2001 21:39:07 -0400*

I recently received a new AT&T Universal Card Visa Card. The card came with a security callback activation feature where you call an 800 number and enter your card number. If you are calling from home (and presumably have not blocked the caller ID feature), this call activates the card.

The part of the procedure that surprised me was that after typing in my card number, the voice response system:

- cautioned me to stay on the line until I heard a confirmation that my card was activated
- launched in to 30 second advertisement for a form of disability insurance. The insurance is sold with a 3 month trial period after which the insurance is automatically charged to your card.
- asked me to type "1" to purchase the insurance or "2" to not purchase the insurance

- asked me a second time to to type "1" to purchase the insurance!

- finally, after two "2" responses, the voice confirmed activating my card

Besides being quite annoyed at being solicited in this manner, I had a moment of panic at the first question. Voice response systems that ask you to enter "1" to confirm a request are very common. Was this confirmation request to activate the card or to purchase the insurance? It took a moment of reflection to assure myself that I was saying no to the insurance.

The risks are that one might

- accidentally purchase insurance they don't want
- feel forced to buy insurance in order to activate the card
- hang up too soon and not activate the card

Given the confusion that is often intentionally introduced by creative marketing, mixing advertising and a security procedure seems a very poor practice.

-Bob Green

---

## **🔥 Techs must report child pornography**

"Brien Webb" <bwebb@apexvoice.com>

*Mon, 30 Jul 2001 20:00:02 -0700*

Source: Associated Press

<http://www.washingtonpost.com/wp-srv/aponline/20010727/>

[aponline203146\\_000.htm](#)

In South Carolina, a new law on education standards for day-care workers has a requirement that private technicians tell police if they find child pornography when servicing computers.

Think of the possibilities. You're servicing computers, and you get the idea to have some fun. You take a client's computer, roll the date back, access some child pornography web site(s), reset the date, and call the cops.

Carrying it one step further, imagine that this as a political "dirty trick". It might just be the mayor or some legislative representative who gets victimized.

Who would believe any protestations of innocence?

--Brien Webb

---

## **✶ Re: Dutch government and virtual child pornography (Dinwiddie, R-21.47)**

Christian Reiser <C.Reiser@internet-security.at>

*Mon, 30 Jul 2001 11:53:16 +0200*

A comment to a quite old posting, but it might still be interesting:

George Dinwiddie brought up the issue, how difficult it is, to guess a person's age. This is a problem, when the definition of child

pornography

depends on the age of the person on the picture.

In Austrian legislation the definition of child pornography does not depend on the age of the person, but something is child pornography, when one or more persons involved in pornography look as if they were under 14. This solves the problem of finding out the age, but obviously raises some others.

Christian Reiser, ASSIST, 1190 Wien, Nussdorfer Laende 29-33  
C.Reiser@internet-security.at, priv: Christian@Reiser.at +43 1  
370 94 40

---

## **✶ Re: Super-accurate atomic clock hates Sundays (Knowlton, [RISKS-21.55](#))**

Phil Kos <PhilK@solthree.com>  
*Tue, 31 Jul 2001 17:28:53 -0700*

Ironically enough, when I went to \*The NYTimes\* online to check out the article on AT&T's new speech synthesis software (also mentioned in [RISKS-21.55](#)), I noticed an article on a new type of atomic clock currently under development at NIST. The article quotes Dr. Alan Madej of the National Research Council, Ottawa, as saying "It certainly is a very big advance for atomic clocks."

Presumably the display problems can be fixed now that MS has (finally, after at least three years) fixed the 4/1 DST bug. Or do you suppose the NRC's

display software had their very own equivalent to MS's mis-implementation of DST? After all, any error that can be made once can be made again and again (buffer overruns are a good example).

---

## ✶ What is your area code, really?

Andrew Koenig <ark@research.att.com>

*Sun, 29 Jul 2001 20:00:15 -0400 (EDT)*

This evening, I wanted to connect a laptop to the Internet to download updated virus definition files. I tried placing a call, then realized that I didn't know whether the machine was set up correctly for my present location, so I cancelled the call. After checking the machine, I thought it looked reasonable, so I tried again.

Five minutes later, two police officers showed up at my door, saying that they had received a 911 (emergency) call from my home.

It took me a while to piece together what had happened:

1. Because I wanted to update the virus definition files, I called from "Administrator" rather than from my own account.
2. The last time I dialed out on that machine as "Administrator" was from a hotel room in San Antonio.
3. On the other hand, the phone number to dial for the ISP had since been changed to back home in New Jersey.

4. The default area code for a dial-up connection is 1, which happens to be the same as the country code for USA.

Therefore,

when setting the ISP's phone number, I had mistakenly assumed

that the area code would go along with the phone number and specified an area code of 1 (which I thought was the (correct)

country code of 1) and a phone number of 908 yyy yyyy (instead of yyy yyyy as it should have been).

5. The network dialer, which still thought I was in a hotel room,

dialed 9 (for an outside line), 1 (for a toll call), 1 again

(for what it thought was the area code), and then 908 yyy YYYY

(which was ignored).

I suppose the risks are obvious...

Andrew Koenig <ark@research.att.com>

---

## **✶ Online advertising: Fraud, false positives and a novel DOS attack**

"John O'Connor" <jpoc@hotmail.com>

*Fri, 27 Jul 2001 11:49:15*

There has been some comment, in recent editions of risks, on the subject of online advertising as seen from the perspective of a Web surfer.

From the viewpoint of a Webmaster seeking ad income, there are some interesting aspects including what seems to be a novel form of DOS attack.

I'll focus on one particular advertising model known as Cost Per Click or CPC.

In this mechanism, a Web site will display a banner for an advertiser and, when a surfer clicks on the banner, the advertiser will pay a small sum to the publisher of the Web site. Thus the publisher will receive an income dependent on the CPC multiplied by the Click Through Ratio or CTR.

A simple click may cost an advertiser somewhere between two and fifty US cents and there is normally an agency of some sort between the two parties to see fair play, count the clicks, handle payments etc.

One fairly obvious risk is that an advertiser who wants brand awareness and not clicks can get free advertising by running ads that will not get clicked but which will enhance brand recognition.

From the advertisers viewpoint, fraud is the main risk. A Web site owner may use an automated system to generate bogus clicks to claim money that was not properly earned. There are thousands of http proxy servers that suffer from the same weakness that allows spam e-mail to exploit open smtp relays. Using these, a Web site owner bent on fraud can generate thousands of bogus mouse clicks.

Of course, advertisers or, more commonly, the agencies with whom they deal take whatever steps they can to combat such fraud. One route used by many is just to have a cut off point for the CTR and say that a Web site

with a high CTR will be automatically barred for fraud. Clearly this leads to the normal risk of false positives where a legitimate site with a high CTR is excluded. Interestingly, the false positives will here work to exclude the sites which are the best ones for the advertiser to use. For example, suppose that a dating agency, specialising in women from Russia seeking men from the West, uses an agency to run its banner ads on the Web sites represented by the agency. Most of the time, such ads will attract a CTR of about 0.2%. But what if one of the sites in the ad agency network happens to specialise in advice on exactly this topic? (Fiancee visas, how to address a letter to a country the uses the Cyrillic alphabet etc.) That site may see a CTR of over 5% which will rapidly earn it exclusion for fraud. Of course, that is exactly the site on which the advertiser would like to run its ads.

And the novel DOS attack?

Recent reports on the Web publisher forums at [geekvillage.com](http://geekvillage.com) have focussed on another problem. Suppose that two sites are in competition as they cover the same subject area and target the same pool of surfers and advertisers. Site A runs banner ads and site B would like to get those ads for itself and perhaps even close down site A and get the surfers too. The operator of site B could set up a click-bot to cause open proxy servers to send thousands of clearly false clicks to the advertiser: seemingly on behalf of site A. Site A will soon be flagged for fraud and will lose its advertising income and

may well close.

John O'Connor <http://www.jpoc.net>

---

**✶ Re: Even a fatal error can't kill it (Haynes, [RISKS-21.53](#))**

Terry Brugger <zow@torii.bruggerink.com>

*Sun, 22 Jul 2001 10:45:38 -0700*

I recently had a similar experience with Ticketmaster's on-line ordering system. I was buying a ticket to a show by my favourite artist as soon as the tickets went on sale (I wanted a good seat). Unfortunately, the group has MANY other fans in the Bay Area, so the system was quite sluggish and timed out frequently. I selected the seat I wanted, entered in all my info and submitted it. After waiting a minute or two it came back with an error message to the effect of, "Unable to confirm your order - hit the back button and resubmit it." When I did so I was informed that my session timed out and that I should try again from the beginning. So I did, five times before the order went through and was confirmed. Everyone knows what happened next: I ended up with five tickets. Ticketmaster was nice enough about it, but I was still left with the task of mailing them the unwanted tickets in order to receive my refund.

The risk: If you're going to build a system with the primary task of selling tickets to popular events:

1. Make sure it can handle the load when those events go on sale and
2. Make sure it correctly reports on the completion of transactions.

"Zow" Terry Brugger <zow@acm.org> <http://bruggerink.com/~zow>

---

## ⚡ Re: Even a fatal error can't kill it ([RISKS 21.53](#))

Joe Thompson <joe@orion-com.com>

*Thu, 19 Jul 2001 23:45:44 -0400*

jhaynes@alumni.uark.edu noted in [RISKS 21.53](#):

> No doubt there are other systems out there which have the possibility of  
> completing a transaction and then telling the user that there has been a  
> fatal error. Maybe a whole lot of them.

I recently had just such an incident with my bank (Chevy Chase Bank, based in Maryland). I used the online banking tools to transfer some funds from one account into another. Later that day I had a need to stop payment on a check, so again I logged on and transferred enough money back into the first account to cover the stop-payment fee.

Later that night I withdrew some funds from the second account at an ATM, and my receipt showed the correct balance. The next night I did the same (total withdrawals \$60.00 for the 2 transactions). The following day at lunch I tried to make a withdrawal at an ATM and was denied --

with the  
receipt showing a balance of approximately -\$60.00 in the second  
account!

You guessed it -- the online transfers I made had disappeared  
from the  
system, and my balances had "snapped back" to what they would  
have been had  
they never happened.

Chevy Chase customer support, fortunately, believed me (in part  
because  
it's impossible to have a negative balance in a savings account  
without  
some really odd goings-on), and later that week it turned out to  
be a good  
thing because the chaos of those few days resulted in two checks  
that were  
currently going through the system "bouncing". CC refunded my  
insufficient-  
funds fees -- and the payees never knew because the two payments  
were made  
via Chevy Chase online payment, which sends the equivalent of a  
cashier's  
check (it can't bounce).

The RISK, of course, is the old story: adding new systems adds  
complexity  
and can have entirely unexpected results. -- Joe

---

## **⚡ Re: Even a fatal error can't kill it**

"John M. Hayes" <john.hayes@marconi.com>

*Fri, 20 Jul 2001 10:59:35 -0400*

The software that prevents duplicate transactions can be a  
problem in and of  
itself. I recently attempted to make hotel reservations through

an online travel agency. On this particular site, there was no provision for reserving multiple rooms. So after making the first reservation, I went back and attempted to reserve a second room. The watchdog software would not allow me to reserve a second room in my name. I ended up having to use a different name in order to make a reservation for the second room. Eventually, this website does allow you to consolidate multiple reservations, but that was not at all clear as I struggled with their system.

Note: For the trip home, I decided to just phone the hotel directly and talk to an operator in order to make similar reservations. It was MUCH easier.

John Hayes (john.hayes@marconi.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 21: Issue 58**

**Thursday 9 August 2001**

## Contents

- [Half of Norway's banks offline for a week: erroneous keystroke](#)  
[Nicolai Langfeldt](#)
- [Danish police break "Safeguard" encryption program in tax case](#)  
[Bo Elkjaer and Jay D. Dyson via Declan McCullagh](#)
- [E-Divorce banned in Singapore](#)  
[Dave Stringer-Calvert](#)
- [Omron uses GPS to catch a car thief](#)  
[Monty Solomon](#)
- [Corrupt Michigan cops abuse police database to stalk, harass](#)  
[Ed Walker via Declan McCullagh](#)
- [OT: rot13, practical uses of](#)  
[Joe Manfre](#)
- [GA scholarship info exposed](#)  
[Rachel Slatkin](#)
- [DoCoMo and thttpd: i-mode DDoS attack!](#)  
[Jef Poskanzer via Dug Song](#)
- [Low-grade cryptography](#)  
[Gene Wirchenko](#)
- [Automated traffic-camera system has flaws](#)  
[Dave Kinswa](#)

- [Risks of the Passport Single Signon Protocol](#)  
[Monty Solomon](#)
  - [Hotmail catches Code Red](#)  
[Brian McWilliams via Dave Farber](#)
  - [Toll Road Transponders used to steal food at McDonald's](#)  
[Arthur Kimes](#)
  - [More Adobe plastering](#)  
[Peter Wayner](#)
  - [Re: WinXP blocks some versions of some programs](#)  
[Michael Loftis](#)
  - [Workshop on Trustworthy Elections](#)  
[David Chaum](#)
  - [REVIEW: "Computer Security Handbook", Hutt/Bosworth/Hoyt](#)  
[Rob Slade](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

## ✶ Half of Norway's banks offline for a week: erroneous keystroke

Nicolai Langfeldt <janl@linpro.no>  
Tue, 07 Aug 2001 13:50:31 +0200

[http://www.digitoday.no/dtno.nsf/pub/dd20010807092448\\_er\\_28707255](http://www.digitoday.no/dtno.nsf/pub/dd20010807092448_er_28707255)  
(in Norwegian)

This is a mix of abstracting the above article and whatever has been on the news the last few days, and one or two of my own comments:

EDB Fellesdata AS runs the computer services of about half of Norway's banks. On Thursday 2 Aug 2001, they apparently installed about 280 disks in their Hitachi storage. Then, instead of initializing the new disks, they initalized all their disks -- thereby wiping out the entire warehouse.

EDB Fellesdata itself declines to make any statements in the case pending further contact with their customers, the banks. They are considering lawsuits, but if one of their own employees made a "user error", they may have a hard time of it.

Talk about a lot of eggs in one basket, one can only imagine how many terrabytes of database this is, considering the number of disks, and how long it takes to restore from backup, and how many transactions were waiting to be processed from \_other\_ banks once the restore is done. Apparently the computers were running by Sunday, card services and ATMs were available on Monday, but Internet banking and automatic-phone-banking access is limited. They have announced that updated account balances will not be available until Wednesday, the 7th day after the mishap. The concerned banks' customers could pay their bills by visiting a local branch office the whole time, but apparently the transactions had not been processed because creditors have been warned that money may be late in arriving (but presumably retro-credited once the transaction is processed?).

Some information gotten from the only available statement from EDB Fellesdata at

[http://www.edb.fellesdata.no/edb/nyheter/2001/06\\_08\\_driftstans.asp](http://www.edb.fellesdata.no/edb/nyheter/2001/06_08_driftstans.asp),  
also Norwegian.

---

## ✶ Danish police break "Safeguard" encryption program in tax case

Declan McCullagh <declan@well.com>

Thu, 9 Aug 2001 11:24:35 -0400

[From the cryptography mailing list. --Declan; lightly-PGN-ed for RISKS]

> Date: Tue, 7 Aug 2001 22:51:08 +0200

> From: bo.elkjaer@eb.dk

> Subject: Utimacos Safeguard Easy broken by Danish police in tax evasion case

> The German encryption program Safeguard Easy has been broken by the Danish

> police. Today the police from the city Holstebro in Jutland presented

> evidence in court, that was provided after breaking the encryption on five

> out of sixteen computers that where seized april 25 this year.

> All 16 computers were protected with Safeguard Easy from the german

> encryption provider Utimaco. It is not known whether DES, 128-bit IDEA,

> Blowfish or Stealth was used as algorithm on the computers. All four

> algorithms are built in Safeguard Easy. Details are sparse. It is not

> known how the encryption was broken, whether it was brute forced or flaws

> in the program was exploited.

> The computers where seized from the humanitarian (leftwing) foundation

> Tvind (Humana) in connection with a case about tax evasion. Among the

> evidence provided from the encrypted computers were e-mails sent among the

> leaders of the foundation, Poul Jorgensen and Mogens Amdi Petersen

> describing transfers of large sums of money.

> Apparently, but not confirmed, British Scotland Yard has been  
> involved in  
> breaking the encryption. The Danish police doesn't have the  
> capacity to  
> break encryption by themselves. Neither has the Danish civilian  
> intelligence service. Routine is that cases concerning  
> encryption is  
> handed over to the Danish defence intelligence service DDIS.  
This  
> procedure has been described earlier this year by the Danish  
minister of  
> justice in connection with another case. DDIS denies  
involvement with the  
> Tvind case.

> Employees and leaders at Tvind has denied handing over their  
passwords to  
> the computers. One even wrote a public letter mocking the  
chief of police  
> in Holstebro, describing how he changed his password weekly,  
and stating  
> that he'd probably even forgotten his password by now. At a  
time, the  
> police considered putting employees in custody until passwords  
were handed  
> over.

> Bo Elkjaer, Denmark

[followed by a response]

> Date: Tue, 7 Aug 2001 16:25:03 -0700 (PDT)  
> From: "Jay D. Dyson" <jdyson@treachery.net>  
> Subject: Re: Utimacos Safeguard Easy broken by Danish police  
in tax evasion case

> If the OS used was Windows, it's quite likely that the  
plaintext and/or  
> passphrases were recovered in the Windows swap file. Barring  
OS  
> considerations, it's also possible that the police put a  
keystroke logger

> on the system, just as the FBI here in the States did with an  
> organized  
> crime suspect.

> My gut sense is that, since only five of sixteen systems were  
> "cracked,"  
> it seems likely that it was the swap file that let the cat out  
> of the bag.  
> Even so, a flaw in the cryptosystem should be investigated and  
> proven or  
> ruled out.

> Let us not also forget that people can be pressured to divulge  
> passphrases. Rubber-hose cryptanalysis isn't just a humorous  
> concept.

> Jay D. Dyson - jdyson@treachery.net

FROM POLITECH -- Declan McCullagh's politics and technology  
mailing list

You may redistribute this message freely if you include this  
notice.

To subscribe, visit <http://www.politechbot.com/info/subscribe.html>

This message is archived at <http://www.politechbot.com/>

---

## ✈ E-Divorce banned in Singapore

Dave Stringer-Calvert <dave\_sc@csl.sri.com>

Wed, 08 Aug 2001 20:36:36 -0700

SMS (short-text messaging) enables short messages from one cell  
phone to  
another. Muslim authorities had previously permitted men to  
divorce their  
wives by SMS. In April to June 2001, 16 divorces were so  
reported.  
However, now the Islamic Religious Council of Singapore (MUIS),

the Syariah

Court and the Registry of Muslim Marriages are "unanimous in their view that

divorce through SMS is unacceptable. ... Only a judge can confirm a divorce

after deciding that there is merit in the complaint filed by the couple with

the Syariah Court." [Source: Singapore bans text-message divorce, CNET

News.com, 8 Aug 2001; PGNed without comment]

<http://news.cnet.com/news/0-1005-200-6815505.html>>

---

## **Omron uses GPS to catch a car thief**

<Monty Solomon <monty@roscom.com>

*Mon, 6 Aug 2001 01:55:35 -0400*

Omron Corp. plans to deliver your stolen car, and the wretched villain

inside it, right to the nearest koban (Japanese police box).

"Imagine that

someone steals your car, and a network of sensors in the vehicle knows the

person driving is not the right person. So using its GPS, it makes the car

stop outside the nearest koban and locks the driver inside. This is what I

imagine, this is the next stage," said Shin'ichi Mukaigawa, an engineer at

Omron's business incubation center, who has designed the basic elements for

such a system. [Source: article by Paul Kallender, \*EE Times\*, 12 Jun 2001,

<http://www.eetimes.com/story/technology/OEG20010612S0059>]

[Quite few of you noted this item. OCSchwar@MIT.edu added:

How RISKy. How lovely. Hijack someone's car using this system,

park it next to an empty koban, and let the Yakuza do their thing.

PGN]

---

## **✶ Corrupt Michigan cops abuse police database to stalk, harass**

Declan McCullagh <declan@well.com>

*Sun, 05 Aug 2001 11:59:48 -0400*

[According to the third Detroit Free Press story, a cop who stalked a woman using his access to police databases was "suspended for a day without pay."

That'll teach 'em! --Declan] [FROM POLITECH]

> Date: Sat, 04 Aug 2001 02:08:36

> From: "Ed Walker" <ed\_walker@hotmail.com>

> Subject: Michigan cops abusing database

> [www.governing.com/news](http://www.governing.com/news) had a link to a freep article that may be of

> interest to politechnicals. The first two links are the story, and the

> third is an account of a truly creepy cop stalking someone he met while on

> duty.

> Michigan Newspaper: Police Abuse Database Police throughout Michigan,

> entrusted with the personal and confidential information in a state law

> enforcement database, have used it to stalk women, threaten motorists and

> settle scores. Over the past five years, more than 90 Michigan police

> officers, dispatchers, federal agents and security guards have abused the

> Law Enforcement Information Network, according to a Detroit Free Press

> examination of LEIN records and police reports. More: Detroit  
Free Press  
> [http://www.freep.com/news/mich/lein31\\_20010731.htm](http://www.freep.com/news/mich/lein31_20010731.htm)  
> [http://www.freep.com/news/mich/lein1\\_20010801.htm](http://www.freep.com/news/mich/lein1_20010801.htm)  
> [http://www.freep.com/news/mich/amber31\\_20010731.htm](http://www.freep.com/news/mich/amber31_20010731.htm)  
  
> Ed Walker

---



Joe Manfre <manfre@flash.net>  
7 Aug 2001 20:23:21 GMT

Subject: OT: rot13, practical uses of

[Contributed by Mark Brader. PGN]

Recently there has been some discussion on AUE of the many  
fascinating  
ways in which the venerable letter-substitution scheme called  
"rot13"  
can be used. Well, this article may be of some interest:

<http://www.zdnet.com/zdnn/stories/comment/0,5859,2800985,00.html>

It deals with a certain Russian cryptanalyst who has been jailed  
for  
cracking and exposing the encryption schemes that some  
electronic book  
publishers use to protect their copyrighted properties. Turns  
out that one  
publisher of industrial reports was using rot13 to protect its  
valuable (to  
the tune of \$3,000 a pop) works.

Joe Manfre, Hyattsville, Maryland.

## **GA scholarship info exposed**

Rachel Slatkin <rslatkin@pobox.com>

Wed, 8 Aug 2001 09:25:03 -0400

Computer passwords and personal information about participants in Georgia's HOPE scholarship program were inadvertently exposed on the web as early as December 2000. The information was apparently cached by several search engines, including Google. From the \*Atlanta Journal Constitution\*, 8 Aug 2001, "State staff may feel byte from hackers":

"Last Nov. 14, he said, a member of the agency's technical staff copied a file onto the HOPE computer system that prevents Internet search engines from indexing the system's contents.

But another program in the system deletes unused files after 30 days, Newsome said. So about Dec. 15, the security file was wiped out, exposing other files."

It's not clear what "security file" was accidentally removed. The news articles I've read about this have not named the file. I'm guessing it was either robots.txt or .htaccess, hopefully the latter.

Many system administrators have discovered the risks of deleting "unused" files without being sure of their purpose. Having the procedure happen automatically compounds the problem.

Rachel Slatkin rslatkin@pobox.com <http://pobox.com/~rslatkin/>

## 🔥 DoCoMo and thttpd: i-mode DDoS attack!

Dug Song <dugsong@arbor.net>

Thu, 2 Aug 2001 20:06:05 -0400

Poor jef has become the victim of his own success (and DoCoMo's)! Perhaps this qualifies as the first cellphone-based (i-mode) distributed denial-of-service attack? :-/

Dug Song, Security Architect, Arbor Networks, Inc.

Date: Thu, 02 Aug 2001 11:22:14 -0700

>From: Jef Poskanzer <jef@acme.com>

To: thttpd@bomb.acme.com

Subject: [THTTPD] DoCoMo and thttpd

Hey, is anyone on the list familiar with DoCoMo? Apparently it's a type

of cell-phone / web browser device from Japan. I have suddenly started

getting a [whole] lot of hits to <http://www.acme.com/software/thttpd/> with

various versions of DoCoMo in the user-agent field.

Unfortunately the

referrer field is blank, which makes it difficult to figure out why this is

happening. Current working theory is that some server run by the DoCoMo

company switched over to using thttpd, and I'm getting the usual spillover

from any 404 pages on their site. I've seen this effect before with large

ISPs, but never with such a high volume of hits. My bandwidth is pegged

to the throttle right now, and they're not even fetching the inline images

(which by the way means I'm not getting any ad impressions from these

hits, which is somewhat annoying). [...]

Jef Poskanzer jef@acme.com <http://www.acme.com/jef/>

---

## ✶ Low-Grade Cryptography

Gene Wirchenko <genew@shuswap.net>

*Tue, 07 Aug 2001 22:31:48 -0700*

DMCA and encryption is discussed in this article:

<http://www.zdnet.com/zdnn/stories/comment/0,5859,2800985,00.html>

My favourite part: "Publishers encrypt their books to prevent them from being read by anyone except the registered owner... they hope. But it turns out that the encryption software of at least two manufacturers is so weak that it can be broken instantly. One publisher, Sklyarov found, uses a cypher called rot13 ...". [Doggedly rot-wily? PGN]

---

## ✶ Automated traffic-camera system has flaws

dAVe <kinswa@mail.com>

*Sun, 05 Aug 2001 12:03:57 -0700*

>From the Seattle Times:

[http://seattletimes.nwsourc.com/html/localnews/134326067\\_trafficam05m.html](http://seattletimes.nwsourc.com/html/localnews/134326067_trafficam05m.html)

It was not the kind of "Kodak moment" the city of Lakewood hoped for. Its high-tech traffic camera had just nabbed Cyn Mason for doing 38 in a 30-mph

zone. The camera captured the license plate on the Tacoma woman's car as it sped through a school zone June 8. Or so it seemed.

After receiving a notice, a thumbnail copy of the incriminating image and a demand for \$71, Mason put pen to paper:

"This is my sworn statement, under penalty of perjury, that your system cannot distinguish between the sporty coupe shown in the ticket picture, and the Honda CR-V sport-utility vehicle that I drive. In other words, I swear that you have the wrong car, since the one shown in the ticket is not my vehicle. Is this sufficient to correct your error, or would you like me to swear at you some more?"

---

## ⚡ Risks of the Passport Single Signon Protocol

Monty Solomon <monty@roscom.com>  
*Mon, 6 Aug 2001 22:35:53 -0400*

David P. Kormann and Aviel D. Rubin,  
Risks of the Passport Single Signon Protocol,  
IEEE Computer Networks, volume 33, pages 51-58, 2000.

David P. Kormann and Aviel D. Rubin  
AT&T Labs - Research  
180 Park Avenue  
Florham Park, NJ 07932  
{davek,rubin}@research.att.com  
<http://avirubin.com/passport.html>

Abstract: Passport is a protocol that enables users to sign onto many

different merchants' web pages by authenticating themselves only once to a common server. This is important because users tend to pick poor (guessable) user names and passwords and to repeat them at different sites. Passport is notable as it is being very widely deployed by Microsoft. At the time of this writing, Passport boasts 40 million consumers and more than 400 authentications per second on average. We examine the Passport single signon protocol, and identify several risks and attacks. We discuss a flaw that we discovered in the interaction of Passport and Netscape browsers that leaves a user logged in while informing him that he has successfully logged out. Finally, we suggest several areas of improvement.

---

## **🔥 Hotmail catches Code Red (via Dave Farber's IP)**

Brian McWilliams <brian@pc-radio.com>

*Wed, 08 Aug 2001 18:01:34 -0400*

[From Dave Farber's IP: <http://www.interesting-people.org/> ]

Microsoft's Hotmail Is Red Hot From Worm

Several systems hosting the MSN Hotmail service have been infected by variants of the Code Red worm, Microsoft has confirmed.

<http://www.newsbytes.com/news/01/168837.html>

---

## **✶ Toll Road Transponders used to steal food at McDonald's (Re: R-21.43)**

Arthur Kimes <artki@netzero.net>

Thu, 02 Aug 2001 19:32:39 -0700

> McDonald's customers will wave the "Speedpass" ... at a drive-through window  
(also see [RISKS-21.46](#) and 21.49)

Some toll roads in Orange County, California, do use those transponders (not the Mobil "speedpass") and local McDonald's have been accepting those as payment since April 2000. Since then, according to the Transportation Corridor Agencies, there has been \$4,000 in charges for food at McDonald's using stolen transponders. [Source: \*Los Angeles Times\*, 23 Jul 2001]

---

## **✶ More Adobe plastering (Re: Maggard, [RISKS-21.56](#))**

Peter Wayner <pcw@flyzone.com>

Fri, 3 Aug 2001 09:10:36 -0400

In [RISKS-21.56](#), Michael Maggard writes, "...Adobe has been installing a mysterious file of their own that regularly 'calls home' for reasons unknown."

Perhaps this kind of reporting software is necessary, but it may be the reason why I'm slowly giving up on Adobe products. My version of InDesign

crashes frequently. My version of ImageReady has the strangest bug. If my system has been up for a bit, ImageReady refuses to run. If I reboot, it's fine. I suspect this has something to do with the quick blip of the network access LED on the router that flickers just after starting up. Maybe that little phone-home program doesn't say the right thing to ImageReady. I thought about complaining or investigating, but I decided that making the transition to GIMP is simpler.

This topic has been on my mind while I've been working on creating simple watermarks for a pay-per-copy experiment. (See <http://www.flyzone.com/satstory/> or just end \$.75 to [satstory@flyzone.com](mailto:satstory@flyzone.com) for a copy of a story on DirectTV hacking) I considered complicated encryption mechanisms and gave up. The complexity took too long to develop and excluded too many legitimate customers. In the end, I just insert the purchaser's name in the file on the way out the door.

This kind of watermark may be easy to defeat, but that has advantages. First, bright kids get no boost from hacking the system. It's trivial. But it is still complex enough to require someone to take a positive step to defeat it. If they can live with themselves, well, they'll get enough punishment. Finally, there is no complexity to crash systems and drive users nuts.

---

**✶ Re: WinXP blocks some versions of some programs (Griffin,**

## **RISKS 21.57)**

Michael Loftis <mloftis@wgops.com>

*Tue, 07 Aug 2001 20:33:15 -0700*

They're blocking drivers because too many vendors have been implementing bad code in their drivers.

---

## **⚡ Workshop on Trustworthy Elections**

David Chaum <david@chaum.com>

*Wed, 08 Aug 2001 14:23:15 -0700*

26-29 August 2001, Tomales Bay, California: WOTE (Workshop on Trustworthy

Elections) is a small research-oriented workshop devoted to advancing

technologies for election integrity and ballot secrecy, organized by David

Chaum and Ronald L. Rivest. Topics include: Cryptographic protocols,

computer security, audit, operational procedures, certification, tamper-resistance, document security, integrity, ballot secrecy, voter

authentication, all as related to trustworthy elections.

<http://www.vote.caltech.edu/wote01/index.html>

---

## **⚡ REVIEW: "Computer Security Handbook", Hutt/Bosworth/Hoyt**

Rob Slade <rslade@sprint.ca>

*Tue, 7 Aug 2001 11:07:47 -0800*

BKCMSCHB.RVW 20010530

"Computer Security Handbook", 1995, Arthur E. Hutt/Seymour  
Bosworth/

Douglas B. Hoyt, 0-471-11854-0

%E Arthur E. Hutt

%E Seymour Bosworth

%E Douglas B. Hoyt

%C 5353 Dundas Street West, 4th Floor, Etobicoke, ON M9B 6H8

%D 1995

%G 0-471-11854-0

%I John Wiley & Sons, Inc.

%O U\$90.00 416-236-4433 fax: 416-236-4448

%T "Computer Security Handbook, Third Edition"

Overall, this work appears to be strongly influenced from a time  
when

computers were mainframes locked in glass rooms, and the  
information

technology department was under the jurisdiction of accounting.

Although

some effort has been made to address more recent topics, the  
attempt is

piecemeal at best, and quite limited in depth.

Part one looks at the responsibility of management in the  
security concern.

The first essay, specifying the role of management, certainly  
dates the work

in the big iron era, defining security solely from the  
perspective of

availability. Disclosure of information does get a mention, but  
even the

list of risks to be considered concentrates primarily on  
malfunction or

disaster. A second paper takes a rather vague look at policies  
and related

documents, but is backed up with a number of examples. The  
review of risk

analysis is similarly nebulous, although it does have some  
potentially

useful tables of probable threats. Optimism about the

availability of background information seems to surround the discussion of employee policies, but some important basic principles are presented. Legal issues are dealt with briefly, but over a wide range of topics. The article on computer crime is not particularly realistic: as one example, the examination of controls concentrates on provisions for preventing programmers from installing logic bombs, but the case studies actually cited as examples of the need for such controls were perpetrated as fraud by those in positions of authority.

Part two outlines basic safeguards. Disaster recovery is, again, reviewed primarily from the mainframe perspective. The principles may be the same, but the important resources for a corporation probably involve many more aspects than just a mainframe and data. An overview of insurance sounds very much like a sales pitch, although it does divide the topic up by type of threat, and examines different factors that can affect price and the willingness of the insurers to make good on a loss. (I was amused to note that the section on viruses basically admits that vendors will use extraordinary interpretations of standard wording to weasel out of paying.) The chapter on auditing appears to have been written solely from an accounting perspective, and, while the points listed would be helpful in creating part of a security policy, they address only those issues related to internal fraud. System application controls are discussed strictly in terms of development cycles and ideas such as "total quality management"

(TQM).

Part three moves to physical protection. Hardware protection takes a detailed look at internal error situations right down to the gate level, as well as a more superficial examination of architecture concerns and environmental problems. Accidental calamities are also the major emphasis in computer facility protection, although there is some attention paid to the need to secure cabling. "Monitoring and Control Devices" presents theory behind surveillance and alarm systems.

Part four starts to look into technical aspects of data security. A chapter on software and information security appears to have some valid points to make (aside from the misinformation on viruses) but is written in such a convoluted manner that most material must be read several times to puzzle out the meaning. An essay on records retention has been retrofitted to become an examination of computer data security. The paper on encryption is extremely disjointed (for example, dropping a discussion of network topologies into a purported explanation of the RSA [Rivest Shamir Adleman] encryption algorithm), and almost completely lacking in details. A rather generic security overview (with questionable virus information) is supposed to address data communications and networking. A grab bag of penetration techniques and countermeasures provides some interesting prompts to consider various attacks, but is not organized or complete enough to fully cover the subject. The chapter on viruses and related threats is rife

with errors,  
and confuses the various types of problems with each other as well as with unverified speculation.

Part five deals with special protection issues. Chapter twenty suggests that you might want to be a little careful when dealing with outside contractors. While there is some disorganization, and a few odd anachronisms, the paper on personal computers is much more practical than most of the preceding material. The essay on LANs presents a primer on networks, and then a generic overview of security, without an awful lot of relation between the two. The chapter on Internet security has some basic information, but is quite disorganized.

Supplements are supposedly produced to update the work. Some such documents ask you to replace paragraphs and correct errors: others offer additional sections to enhance the original essays. In the 1997 supplement (ISBN 0-471-17297-9) there are some weak addenda for auditing, encryption, and viruses, as well as a decent, though still disorganized, extension to the Internet material. There is also a first rate examination of e-mail privacy issues and a reasonable though uninspired review of single sign-on. When I contacted the publisher, I was told that the 2000 supplement was still in the editorial stage. In fact, so was the 1998 supplement! So I wouldn't expect any updates for the book in the near future.

Most of the material is fairly obviously old, and originally intended to address topics applicable solely to mainframe computer

establishments, or even non-computerized systems. Patchwork updating is evidently an afterthought. A great deal of material is repeated many times over in different essays. Generally the papers have little detail or depth, so the recapitulations do not add much new content each time.

There is useful material in the work, but it is difficult to abstract the good from the outdated and 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    BKCMSCHB.RVW    20010530  
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 21: Issue 59**

**Friday 10 August 2001**

## Contents

- [Laser eye surgery](#)  
[Henry Baker](#)
- ["You Can't Hide Those Lying Eyes in Tampa"](#)  
[Adam Shostack](#)
- [The Internet park bench](#)  
[Richard Jay Solomon via Dave Farber](#)
- [PDF backward compatibility failures](#)  
[Marc Auslander](#)
- [A lucrative fiasco](#)  
[Brian Randell](#)
- [Risks of automatic verification](#)  
[Geoff Kuenning](#)
- [Possibility of a Warhol Worm: Complete infection in 15 minutes!](#)  
[Nicholas C. Weaver](#)
- [Adobe clarification on spyware article](#)  
[Gunar Penikis](#)
- [Danish police: Safeguard Easy not broken; passwords were weak](#)  
[Bo Elkjaer](#)
- [Re: OT: rot13, practical uses of](#)  
[Rich Wales](#)

- [Re: Georgia scholarship info exposed](#)  
[Phil Kos](#)
  - [Re: Freeware app to retrieve passwords from Internet Explorer](#)  
[Marc Roessler](#)
  - [Mutual authentication - not!](#)  
[Michael Bacon](#)
  - [Re: What is your area code, really? \(](#)  
[Declan McCullagh](#)
  - [Is your phone bill private? Think again...](#)  
[Ted Lee](#)
  - [Re: Firefighter's phone lines disrupted ... SMS hoax](#)  
[Stanislav Meduna](#)
  - [Caller ID "hack" not a hack at all](#)  
[William Kucharski](#)
  - [ANI is NOT Caller ID](#)  
[Danny Burstein](#)
  - [DoCoMo thttpd is not all.net thttpd](#)  
[Fred Cohen](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

## ⚡ Laser eye surgery

Henry Baker <hbaker1@pipeline.com>

*Thu, 09 Aug 2001 13:52:21 -0700*

Someone close to me had laser eye surgery to correct significant near-sightedness two days ago. The surgery apparently went very well, but as I watched the procedure being performed, I was horrified to see two things:

\* the use of Windows as the major interface for this system (www.ladarvision.com), both for the output of the real-time video of the eye, both the tracked and the untracked views, as well as for

the entry

and display of the parameters. Based on my personal experience with

Windows (I reboot on the average of 3-4X per day), I find it almost

inconceivable that someone would trust their eyesight to such a software

disaster area. I wasn't aware that anyone had done any source checking

of the Windows system to make sure that the numbers typed in were properly

interpreted in all cases. Furthermore, even if someone had done such a

check, it is inconceivable that such checks would remain valid for more

than one version of the software. (Getting input routines correct isn't

easy -- I'm aware of popular software systems (non-Windows) that still

contained the same input conversion bugs after almost ten years and 5

versions.)

\* during the entry of parameters, the technician quickly "clicked away"/dismissed a number of error windows of the form

"parameter out of

bounds" -- seemingly on almost every number entered. When error windows

of this type pop up so frequently and are routinely dismissed, it is like

crying "wolf" -- eventually, no one listens even when there is a really

bad problem.

I was, however, very impressed with the quality of the eye-tracking system,

which keeps the laser locked onto the pupil for upwards of 2.5 minutes, with

no noticeable jitter (I would estimate that the jitter was well under a

single pixel out of an image probably 640 pixels wide).

## 🔥 "You Can't Hide Those Lying Eyes in Tampa"

Adam Shostack <adam@zeroknowledge.com>

Wed, 8 Aug 2001 13:03:34 -0400

[http://www.sptimes.com/News/080801/TampaBay/\\_They\\_made\\_me\\_feel\\_li.shtml](http://www.sptimes.com/News/080801/TampaBay/_They_made_me_feel_li.shtml)

is the story of Rob Milliron, whose picture, captured from Ybor city surveillance cameras, was published in US News and World Report. A woman in Tulsa saw his picture and (incorrectly) identifying him as her ex-husband, called the police.

Many of the risks are generally familiar, issues like mis-identification.

Worth asking is why didn't they choose the picture of a criminal who was actually caught? Perhaps because the system does not function as advertised?

---

## 🔥 The Internet park bench (From Dave Farber's IP list)

Richard Jay Solomon <rsolomon@dsl.cis.upenn.edu>

Fri, 10 Aug 2001 13:35:01 -0400

>[http://news.bbc.co.uk/hi/english/sci/tech/newsid\\_1481000/1481783.stm](http://news.bbc.co.uk/hi/english/sci/tech/newsid_1481000/1481783.stm)

Thursday, 9 August, 2001, 13:44 GMT 14:44 UK

Bad start for Internet bench: The teenagers took advantage of the free service

Two teenagers discovered the world's first Internet bench could

be used to  
make free international telephone calls. The cyber-seat, which  
is based in  
a public park in Suffolk, UK, went online on Monday. Neil  
Woodman and Dan  
Sanderson, both 17, took a normal telephone handset along to the  
bench,  
which was created by Microsoft's MSN service in partnership with  
the local  
council. The pair cheekily phoned St Edmondsbury Council to  
warn them of  
the problem and then tried to call Microsoft boss, Bill Gates.

---

## ✶ PDF backward compatibility failures

Marc Auslander <marc@watson.ibm.com>  
*10 Aug 2001 16:50:56 -0400*

I can't read my Vanguard statements (back to 1998) with Acrobat  
5.0. In  
looking at the Adobe site, this is not the only backward  
compatibility  
failure reported.

So what has become a defacto document storage standard may in  
fact leave us  
with documents we can't read!

Marc Auslander <marc@watson.ibm.com> 914 945-4346 (Tieline  
862 Fax x4425)

---

## ✶ A lucrative fiasco

Brian Randell <Brian.Randell@newcastle.ac.uk>  
*Thu, 9 Aug 2001 22:28:45 +0100*

Magistrates courts staff are having to work with two computers on their desks instead of one after being presented with new PCs which do not have the software to do the main job they were bought for. In the latest in a long line of government IT humiliations, the Lord Chancellor's Department is pressing ahead with the installation of new computers in 400 magistrates courts even though delivery of the core application, a new case management system, has been indefinitely delayed. The result is that staff still rely on their old computers - installed 10 years ago - to access the casework system, while using the new PCs only for basic functions such as word processing and e-mail. An investigation by \*Computer Weekly\* has established that by installing the computers, the contractor ICL is now entitled to be paid more than half the contract's 319,000,000 pounds value, despite its failure to deliver the core application. [Source: Court staff hit by IT fiasco; software snag hits magistrates computer project, Stuart Millar, (UK) \*The Guardian\*, 9 Aug 2001]

Full story at

<http://www.guardian.co.uk/internetnews/story/0,7369,534162,00.html>

Dept. of Computing Science, University of Newcastle, Newcastle upon Tyne,  
NE1 7RU, UK +44 191 222 7923 <http://www.cs.ncl.ac.uk/~brian.randell/>

---

## **⚡ Risks of automatic verification**

Geoff Kuenning <geoff@cs.hmc.edu>

*Tue, 7 Aug 2001 17:24:17 -0700*

In the past year or so, a lot of e-shopping sites have installed fraud-prevention software that attempts to verify that you aren't using a stolen credit card. These systems generally operate by comparing the billing address for the card with an address provided by the shopper or with the shipping address for the merchandise.

These systems have caused me endless headaches, because my billing address is a P.O. box in a different state. For some reason, the automated verification system insists on rejecting me with a message indicating that my information doesn't match what's in my bank's records -- despite the fact that I have spoken with the bank to make sure that it is the same. On more than one occasion, I have been forced to resort to telephone calls to get my transaction to go through.

But my favorite was when one site gave me a reject message, so I retried with a slight variation on the address. After a second reject, I got on the phone and straightened it out (without any particular verification requirement, I might add).

That evening, the bank called to ask why I had three charges from the same Web site...

The RISK: programmers who assume that everyone runs their lives the same way

the programmer does. There's an incompetent-programmer RISK here too, but what else is new?

Geoff Kuenning    geoff@cs.hmc.edu    <http://www.cs.hmc.edu/~geoff/>

---

## ⚡ Possibility of a Warhol Worm: Complete infection in 15 minutes!

"Nicholas C. Weaver" <nweaver@EECS.Berkeley.EDU>  
*Thu, 9 Aug 2001 15:11:50 -0700 (PDT)*

Michael Constant and I have performed a basic analysis of a possible worst-case virulence for an active worm like Code Red. By simply changing the infection strategy, a "Warhol Worm" could be developed, able to infect all vulnerable machines in 15 minutes from the moment of initial infection of a single machine!

<http://www.cs.berkeley.edu/~nweaver/warhol.html>

Nicholas Weaver, nweaver@cs.berkeley.edu

[And in Case you have not heard, Code Red III is now operating. PGN]

<http://news.cnet.com/news/0-1003-200-6835996.html>

---

## ⚡ Adobe clarification on spyware article (Maggard, [RISKS-21.56](#))

"Gunar Penikis" <gpenikis@adobe.com>  
*Thu, 9 Aug 2001 13:24:49 -0700*

This is in response to Michael F. Maggard's posting in [RISKS-21.56](#).

I would like to clarify some misconceptions and misinformation that was posted regarding Adobe applications "phoning home". The component in question is AOM, Adobe Online Manager which is included in most Adobe applications.

1. AOM does not scan your computer for registration and product information.

AOM runs concurrently with most applications, it's purpose is NOT to scan for registration and product information and phone home to Adobe. Registration information such as serial number, product name is ONLY sent from the product when the user selects the Registration menu item in the product. This launches the default browser to the registration web page that has product and registration information pre-filled as a convenience (so the customer doesn't have to find the product box, etc.) The serial number is obfuscated in this transaction to protect our customers and Adobe from piracy. Alternatively, customers can print out a registration form, use the registration card, or register via the Adobe.com and type in the product information manually.

2. AOM only sends registration information when you select Online Registration

As I mentioned above, we only send registration information when the user clicks the Registration menu in the product. It is never sent at any other time or with any other interaction.

### 3. Removing any components is NOT recommended.

We highly suggest NOT removing AOM or other files since these components are critical to functionality of the connectivity, collaboration and support features of the product. As part of the regular updates to the products, we are investigating eliminating the dependency of AOM. In the meanwhile, we suggest that users of older products update their version of AOM by selecting Adobe Online and clicking the refresh or update button. Newer product should select the Downloadables or Updates menu item to check for product updates.

What is AOM used for anyway?

AOM stand for Adobe Online Manager. It is core component that coordinates the online interaction between Adobe products. When customers request updated information from within Adobe products by selecting Adobe Online or Updates/Downloadables, AOM processes these requests so that collisions do not occur and the appropriate information is displayed to the user.

I hope this helps clarify some of the concerns your readers have encountered.

Gunar Penikis, Product Manager, Adobe Systems

---

**🚨 Danish police: Safeguard Easy not broken; weak passwords ([R 21 58](#))**

Bo Elkjaer <boo@datashopper.dk>

Thu, 9 Aug 2001 22:18:57 +0200 (CEST)

This is to elaborate and correct the initial mentioning of Safeguard Easy in [RISKS-21.58](#).

It was reported in national media - including tv - that the police had successfully broken the encryption. This, it seems, is not the case. The police have managed to find the passwords of the five encrypted computers. The information concerning the successful decryption of the five computers protected with Safeguard Easy was presented in court by chief prosecutor Poul Gade. Investigation is lead by chief of police in Holstebro, Jens Kaasgaard.

I have just interviewed Jens Kaasgaard. He says:  
'To avoid misunderstandings, we haven't broken Safeguard by technically breaking down the encryption. We have located the passwords in different ways. We have done it like any hacker would have done, by trying to figure out the most probable passwords. This has payed success in five cases.'  
'After doing that we entered the document-parts, the harddisk of the computer. Here we found some of the files unencrypted and other files further encrypted.'  
'When you use Safeguard you put a sort of shell around your data. This is the first part you need to enter. This is what is claimed to be impossible. It is impossible. We have had six private companies looking at this, and they have all failed.'

'We have used completely ordinary police investigation methods.  
We know  
precisely who have had access to the encrypted machines. Then we  
can start  
assessing probabilities and calculate upon this and set up  
models for how,  
if you were a hacker, you'd find your way into the machines.  
That's what  
we have done.'  
You did this yourself?  
'Yes. We did this inside the police system.'

To conclude: Be careful when you choose your password.

Bo Elkjaer

---

## ✉ **Re: OT: rot13, practical uses of (Manfre, [RISKS-21.58](#))**

Rich Wales <richw@webcom.com>  
*Thu, 9 Aug 2001 17:06:52 -0700 (PDT)*

Let's not forget, of course, that when the US Army decided to  
get serious  
about enforcing a "no encryption software" policy on the  
SIMTEL20 archive  
back in 1990, one of the programs that was kicked off the site  
was ... you  
guessed it ... a ROT13 utility.

Rich Wales            richw@webcom.com            [http://www.webcom.com/  
richw/](http://www.webcom.com/richw/)

---

## ✉ **Re: Georgia scholarship info exposed (Slatkin, [RISKS-21.58](#))**

Phil Kos <PhilK@solthree.com>

*Thu, 9 Aug 2001 14:45:08 -0700*

> the security file was wiped out, exposing other files.

I think I would be a bit ticked off if my IT people decided that one of my web servers should automatically be "cleaned" of not-recently-used files, but let's not let that distract us from the real issue.

Rachel hopes that the "security file" was .htaccess. While I can't disagree, I think that it misses the point. Frankly, even .htaccess is not sufficient to protect passwords stored in plain text on an unsecured web server. This is the real problem here. Storing passwords in plain text is an even better-known bad idea than using unchecked buffers on the stack frame, and I hope the person responsible for this piece of phenomenally bad design gets the blame due them.

---

## **✶ Re: Freeware app to retrieve passwords from Internet Explorer**

Marc Roessler <marc@tentacle.franken.de>

*Wed, 8 Aug 2001 17:45:08 +0200*

Now this is interesting. I remember seeing something similar about three or four years ago, named "Snadboy Revelation" back then, worked fine with win95.

I had expected MS to make this more difficult after seeing such a tool..

The RISKS of using password remembering functions are well known, but making revelation of passwords that easy borders the laughable.

Of course, displaying an asterisk for each character of the password is another RISK in itself since it leaks information on the length of the password.. Standard UNIX login does not echo anything at the Password prompt for a reason..

Marc Roessler

---

## ⚡ Mutual authentication - not!

"Michael (Streaky) Bacon" <streaky\_bacon@email.msn.com>

*Tue, 7 Aug 2001 18:58:38 +0100*

I recently received a telephone call from the fraud department at my bank.

I had recently been using a card that I don't normally use and they were just checking that it was still in my possession.

The fraud department asked me to identify myself by giving them my date of birth and 'secret code' that I had supplied years beforehand. They told me what the question was, so I remembered the answer. I declined, and asked them to positively identify themselves to me before I would give them the information. "But we only need to confirm it, I have it on my screen", the lady said. "OK, you tell me what it is and if I agree that's what I told you then I've authenticated you", said I - knowing that it should fail, but

hoping that it wouldn't. "Then you can authenticate me."

After much discussion and calling two supervisors, we agreed that they would tell me the last two purchases I had made on that card (approximately 1 hour and 20 minutes beforehand respectively from two different stores). If they could, then they were probably from the bank, and I would authenticate myself to them. All three people I spoke to said that, "No-one has ever asked us to identify ourselves!"

The RISKS are clear. You supply some 'secret' data to the bank so that they can authenticate you when you call them. But there is no simple way to authenticate the bank when it calls you. You can't ask for the number and call them back, because you have no way of authenticating the number given. They're ex-directory, so you can't confirm it through Enquiries, and they withhold the number so the CLI doesn't show! If you blindly supply the data (as clearly many people do), then you may be divulging to a crook the 'secrets' necessary to authenticate yourself to the bank. The bank has not thought to provide any means of authenticating themselves. I suspect this to be endemic.

Oh, and when I asked what would happen if I refused to authenticate myself -- they said that my card would be suspended "As a precaution." So at least I would know then that it had been the bank I hung up on!

Streaky

## ✂ Re: What is your area code, really? ((Koenig, [RISKS-21.57](#)))

Declan McCullagh <declan@well.com>

*Tue, 07 Aug 2001 21:35:02 -0400*

> Five minutes later, two police officers showed up at my door,  
saying  
> that they had received a 911 (emergency) call from my home.

I had a similar problem this week. I was visiting my parents and helping my mother configure a PC that was last used on a university campus. The PC was still configured for the old area code, and that combined with the "9" prefix that was required to connect to an off-campus dialup gave a dial prefix of "911". (That's the police emergency number, for non-U.S. readers.)

Without knowing how to change the default location -- not a trivial task for a Windows novice -- a person using the computer would have had to edit the dial string every time they tried to connect. Eventually, no doubt, someone would have neglected to do so with results similar to what Andrew experienced.

The risks here are obvious. Unfortunately the obvious fix -- a prompt saying "Do you really wish to dial 911 and call police?" if the location is in the U.S. -- might come as a mild surprise if the user is connecting via an unusual PBX system that may require a "911" prefix.

Declan

## **✶ Is your phone bill private? Think again...**

<TED\_LEE@udlp.com>

*Tue, 7 Aug 2001 15:03:02 -0500*

I suppose this has already shown up and I missed it, but we'll see. I just called ATT's customer service line with a question about my bill. (I don't recall how many menus deep I had to go to get the answer, and even though it was too many, that's not my point.) Somewhere in the process I was asked if I was calling from the number I was calling about and since I wasn't (I was at work) I was then asked to enter the number -- and immediately it came back with a statement about what my bill was and when I'd paid the last one. I have to wonder what other information I might have been able to get without having to authenticate myself in any way.

Ted Lee, Minnetonka, MN

---

## **✶ Re: Firefighter's phone lines disrupted ... SMS hoax ([RISKS-21.55](#))**

Stanislav Meduna <stano@meduna.org>

*Fri, 10 Aug 2001 08:06:33 +0200*

> The cause was a hoax SMS spreading in the network of one of the GSM

> operators stating that it is possible to make free calls using  
this  
> number.

Slowly the details of the case have emerged and - not  
surprisingly -  
revealed another common risk - a risk of not assessing the  
effects of a  
software change, even if it is fixing a simple bug.

There really was the possibility to make free calls. Let zzz  
be the  
emergency number. If you called zzz, the call was properly  
routed. If you  
called zzzyyyyyy, a software bug caused zzz to be stripped and  
the call was  
routed to yyyyyy instead. Charging software looks at the  
beginning of the  
number and have seen an emergency number, so such call was not  
billed.

Then the operator fixed the bug and the fix was analogous to  
plain old  
telephone - ignore remaining digits. Suddenly, all of such calls  
ended at  
the firefighters.

So we are back to software development basics: specify handling  
of an  
invalid input, test the handling and think before you make a fix  
public. The  
fix was good enough for the billing department, but caused  
massive problems  
somewhere else.

---

## **🔥 Caller ID "hack" not a hack at all ([RISKS-21.51](#))**

"William Kucharski" <kucharsk@mac.com>

*Mon, 23 Jul 2001 22:52:16 -0600*

In [Risks 21.51](#), Alexandre Pechtchanski wrote of receiving a phone call with "hacked" Caller ID information. In fact, it is likely no such "hack" occurred, nor is a hack necessary.

Caller ID, (actually CNID, Calling Number ID), is based on data that is sent on trunk lines along with other SS7 signalling data in a phone system. For home users, this information is normally the originating phone number for the call, as that is how your local telco has their switches set up.

Things are a bit different for PBX (Private Branch Exchange) systems, typically found in businesses. They feed directly into telco trunk lines, and the systems are responsible for feeding their own CNID information into the telephone network.

Most newer PBXs can be programmed to either send along the originating phone number of a call or to send a single pre-programmed piece of information. As an example, a company may want the same information sent (say the company name and their main incoming phone number) on all outgoing lines so those receiving calls from the company see the company name and number rather than the number corresponding to the actual outgoing phone line used to place the call.

This is all perfectly OK, as CNID data is not and was never designed to be secure, and is not used for anything but caller ID services.

In Alexandre's case, it's likely a telemarketer either just

programmed a  
nonsense number into their PBX, or perhaps their PBX came  
preprogrammed from  
the vendor with a "sample" phone number in place (e.g. "John Doe  
(212)  
555-1212".)

Note that there is a completely different system, ANI (Automatic  
Number  
Identification), that is used when it is important a caller be  
properly  
identified. It is ANI information that is used to generate phone  
billing records and to provide calling number identification for  
911 services.

(For the security conscious, ANI information is also NOT  
blockable, and  
most phone companies offer real-time ANI to their toll-free  
customers. This  
means that even if you have "Caller ID blocking," if you call a  
company  
using their toll-free number, they will have your phone number  
pop up  
on their screen when the phone rings on their end or will  
receive it in their  
end-of-month statement. This has been ruled fair, as THEY are  
paying for the  
phone call, thus they have a right to know who is calling them.)

The real RISK here is trusting a system that was never designed  
to be even  
remotely secure as a source of accurate information as to the  
identity of a  
caller...

William Kucharski <kucharsk@mac.com>

---

**✶ ANI is NOT Caller ID (Re: Green, [RISKS-21.57](#))**

danny burstein <dannyb@panix.com>

*Tue, 7 Aug 2001 21:03:13 -0400 (EDT)*

This brings up the reminder that Caller Name/Number ID (CNID) is NOT the same thing as Automatic Name/Number Identification (ANI).

The former, which is what is used by (the vast majority of) homes and "regular" (non "800") business lines, can be blocked by the caller on either a permanent per-line basis, or as a choice per-call. (Usually by prepending a special code, generally "\*70", before dialing out).

The latter, which is in use internally by the telcos and by businesses with (so-called) toll-free (1-800/888/877/866, and soon 855) numbers, can NOT be blocked by the caller. Adding in the blocking prepend will NOT have any effect.

So... whenever you reach out to a tollfree number, the recipient of that call *will* get your phone number. Which, of course, lets them kick it through a database for all sorts of other purposes. Sometimes, as in this case, namely credit card receipt verification, a perfectly valid and legitimate one.

The RISK: having just enough knowledge (about blocking CNID) to believe you're keeping info (your phone number) private when no such thing is happening.

---

## ⚡ DoCoMo thttpd is not all.net thttpd (Re: Poskanzer, [RISKS-21.58](#))

Fred Cohen <fc@all.net>

*Fri, 10 Aug 2001 07:23:10 -0700 (PDT)*

It should be noted that this is not the 'thttpd' from all.net that provides secure Web services...

Fred Cohen  
fax:925-454-0171

fc@all.net  
[www.unhca.com/](http://www.unhca.com/)  
<http://all.net/>

tel:925-294-2087

Fred Cohen & Associates.....tel/

The University of New Haven.....[http://](http://www.unhca.com/)

Sandia National Laboratories....



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 21: Issue 60**

**Friday 17 August 2001**

## Contents

- [Heart-device recalls](#)  
[PGN](#)
- [Runway incursions](#)  
[Andres Zellweger](#)
- [Cingular wireless goes down in heat wave](#)  
[PGN](#)
- [Swisscom Mobile breaks down for 10 hours](#)  
[Andre Oppermann](#)
- [Marines face charges in Osprey records falsifications](#)  
[PGN](#)
- [Woman stalked by Michigan cop via police databases is murdered](#)  
[Declan McCullagh](#)
- [Video crypto standard cracked?](#)  
[Monty Solomon](#)
- [Free hotel reservations canceled](#)  
[Steve Bellovin](#)
- [Interstate car tags to be photographed and tracked](#)  
[Steve Holzworth](#)
- [Hacked caller ID?](#)  
[Andrew Hilborne](#)

- [Risks of letting MS not-so-Hotmail do your junk filtering...](#)  
[Michael Loftis](#)
  - [GPS-guide in car going nuts?](#)  
[Martin Schulze](#)
  - [The risks of not verifying e-mail addresses](#)  
[Doug Winter](#)
  - [Re: Mixing advertising and credit-card activation](#)  
[Sam Garst](#)  
[Joel Garry](#)
  - [REVIEW: "The Internet Security Guidebook", Juanita Ellis/Timothy Speed](#)  
[Rob Slade](#)
  - [Dependability and "Open Source" development](#)  
[Cliff Jones](#)
  - [CFP2002: Call for Proposals](#)  
[Lance J. Hoffman](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

## ⚡ Heart-device recalls

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

*Thu, 16 Aug 2001 9:35:51 PDT*

A study from Brigham and Women's Hospital in Boston in the JAMA reports that, over the ten-year period ending Dec 2000, 42 recalls and 10 safety alerts were issued for pacemakers and implantable cardioverter defibrillators (ICDs, as In Cheney, Dick) involving more than 520,000 devices. Over 600,000 Americans have pacemakers and 150,000 have ICDs, so that represents a remarkably high percentage. However, only a small fraction of the recalled devices were actually defective. If recall recommendations were followed, the study estimates that 36,000 devices would

have been replaced. Only a few deaths were attributed to malfunctions.

Advisories are increasing, but that is attributed to increased manufacturer

vigilance and richer information output by the devices.

[Source: article by

Kenneth Chang, \*The New York Times\*, 15 Aug 2001, Natl. Edition A12; PGN-ed]

---

## ✶ Runway incursions

Andres Zellweger <azellweg@hq.nasa.gov>

*Wed, 15 Aug 2001 10:54:24 -0400*

A 14 Aug 2001 Reuters item, New glitch for US system to avoid runway

collisions, talks about more delays in the long promised FAA

Runway

Incursion System -- due to ``excessive false alarms''. This raises an

interesting dilemma for designer of such safety systems. The state of the

art in runway incursion systems is not good enough to detect all potential

incursions without a relatively high level of false alarms.

One could tune the system to have false alarms at an

``operationally

acceptable'' level, but the likelihood of missing some potential incursions

increases. Critics argue that one should not be implemented a system that

misses some potential incursions because air traffic controllers would

become dependent on the system instead of using it a safety net.

Therefore,

they argue, there might be more incursions than if controllers were doing

their job properly without the system in place. Others (and I

fall in this  
camp) think that, with proper training, controllers will not be  
lulled into  
a false sense of security, and safety can be increased when a  
safety net  
that is not perfect is present. I don't think that any air  
traffic  
controller takes his/her job of separating aircraft less  
seriously because  
of TCAS!

Andres G. Zellweger, PhD, NASA code R, 300 E St, SW,  
Washington, DC 20546-0001 1-202.358.0544 azellweg@hq.nasa.  
gov

[The chairman of the relevant House subcommittee on aviation  
suggested  
that the FAA should take the time to get it right. (The  
program is  
already six years behind schedule.) Runway safety is an  
increasing  
with more near misses, including one at Dallas in May 2001.  
LAX and  
O'Hare each had five near misses from 1997 to 2000. PGN-ed]

[This morning's news reports noted a new runway crossing  
near-miss,  
preliminarily blamed on air-traffic control. PGN]

---

## **✶ Cingular wireless goes down in heat wave**

"Peter G. Neumann" <neumann@csl.sri.com>  
*Fri, 10 Aug 2001 14:17:48 PDT*

A little reverse Rube Goldberg: The heat wave in the DC area  
caused a power  
outage, the backup batteries failed, and the automatic system  
that should

have cut over to the backup generator also failed, resulting in disruption of cell-phone service to 301- and 202-area Cingular Wireless customers. The failure of a single switch that was supposed to transfer from batteries to generator power (which was designed to operate autonomously for at least a month) was apparently the ultimately limiting factor. But the generator ran fine! [Source: Associated Press article by Derrill Holly, AP 10 Aug 2001; PGN-ed]

---

## **⚡ Swisscom Mobile breaks down for 10 hours**

Andre Oppermann <oppermann@telehouse.ch>

*Sun, 12 Aug 2001 13:03:15 +0200*

On Friday, July 27th 2001, the whole Swisscom Mobile GSM network, serving 3.3 million customers (70% market share in Switzerland), broke down for 10 hours from approx. 12:30 until 22:30 GMT+0200.

Two independent software errors in the primary and backup network signaling processors (the SS7 network) caused a halt for the processing of all signaling in a GSM network. This includes call setup, call receiving, SMS (short message service), logging onto network and basically everything else. The central GSM systems (HLR, VLR, NMC and so on) stayed up but were unable to communicate with the base stations in the field.

The primary system suffered a complete failure (software error) and as

designed the backup system took over. While it was working fine first the backup system got loaded more and more, judging from the description something like a missing free() call, and eventually broke down too half an hour later.

The newspaper "Le Monde" was reporting insider information last week saying that these signaling processors are made by Alcatel and that Alcatel found out about the software errors two weeks before (and probably also had a fix) but "forgot" to inform Swisscom Mobile about it. Alcatel is now facing a Swiss Franc 30 million liability case. This is the loss Swisscom Mobile has because of lost revenues, not including public image damages.

In one thing I have respect for Swisscom; They did a pretty good job with public relations and informed the media and public very openly about their technical problem(s). Now, two weeks later, Swisscom Mobile also issued a, thought written for the non technician but pretty detailed, press release of the cause and events of this network failure.

Although one funny thing happened; The press release in German is the original one and while translating into English they forgot one just one word but it makes a somewhat significant difference. In the German version it reads "Technical systems do \*not\* guarantee 100% availability [but we do our best to get 99.95%]. In the English version it reads "Technical systems guarantee 100% availability [but we do our best to get 99.95%]". But see yourself:

[http://www.swisscom.com/gd/information/press\\_releases/2001/natel\\_disruption-de.html](http://www.swisscom.com/gd/information/press_releases/2001/natel_disruption-de.html) in German  
[http://www.swisscom.com/gd/information/press\\_releases/2001/natel\\_disruption-en.html](http://www.swisscom.com/gd/information/press_releases/2001/natel_disruption-en.html) in English

Andre Oppermann

---

## **⚡ Marines face charges in Osprey records falsifications**

"Peter G. Neumann" <neumann@csl.sri.com>  
*Fri, 10 Aug 2001 13:09:55 PDT*

Eight Marine Corp officers have been charged with misconduct with the alleged falsification of MV-22 Osprey tilt-rotor maintenance records.

[<http://www.washingtonpost.com/wp-dyn/articles/A59345-2001Aug10.html>]

[See [RISKS-21.14](#), 21, 24, 31, 33, 36, 38, 41 for Osprey problems.]

---

## **⚡ Woman stalked by Michigan cop via police databases is murdered**

Declan McCullagh <declan@well.com>  
*Fri, 10 Aug 2001 10:35:36 -0400*

A Michigan State Police detective whose estranged wife was shot dead at the Potter Park Zoo admitted using police databases such as the Law Enforcement Information Network (LEIN) to check on his wife and her

acquaintances before

her fatal shooting. [Source: \*Free Press\*, 8 Aug 2001; PGN-ed  
[http://www.freep.com/news/mich/lein8\\_20010808.htm](http://www.freep.com/news/mich/lein8_20010808.htm)]

---

## ✶ Video crypto standard cracked?

Monty Solomon <monty@roscom.com>

*Wed, 15 Aug 2001 01:17:48 -0400*

Noted cryptographer Niels Ferguson says he's broken Intel's  
vaunted

High-bandwidth Digital Content Protection (HDCP) Digital Video  
Encryption

System, but fear of U.S. law is keeping him silent on the  
details. HDCP

connects digital cameras, high-definition televisions, cable  
boxes, and

video disks players. [Source: Article by Ann Harrison, 13 Aug  
2001, PGN-ed;

<http://www.securityfocus.com/news/236>]

[Intel has not threatened him, but he can still be sued by the  
U.S. Govt

under DMCA, or by the motion-picture industry. His comments  
are at

<http://www.macfergus.com/niels/dmca/index.html>

Knowledge that it is (or might be) breakable is likely to  
result in other

folks doing it, and perhaps posting it anonymously in some non-  
US Web

site. The globalization of the Internet is clearly going to  
be an

increasingly difficult problem for industries trying to defend  
information

supposedly protected under flawed standards. PGN]

## **✶ Free hotel reservations canceled**

Steve Bellovin <smb@research.att.com>

*Tue, 14 Aug 2001 11:56:40 -0400*

We have here a story of sequential bugs, or at least odd behavior.

Last March, someone entered a rate of \$0 per night for the Mexico City Airport Hilton into an online reservation system. A number of users of the Travelocity web site saw it and reserved rooms. Hilton eventually agreed to honor that rate for one night, and let travelers stay additional nights at "the lowest available rate". But the story has gotten stranger.

According to today's Wall Street Journal, at least two people who made such reservations via Travelocity have found that their reservations have been canceled without their knowledge. Hilton and Travelocity deny any knowledge of what happened. Both cancellations were via telephone calls to Travelocity, made within minutes of each other.

Steve Bellovin, <http://www.research.att.com/~smb>

---

## **✶ Interstate car tags to be photographed and tracked**

Steve Holzworth <sch@unx.sas.com>

*Thu, 9 Aug 2001 19:00:48 -0400*

>From WRAL.com (excerpted):

<http://www.wral.com/news/910501/index.html>

[Charlotte, NC]

... The cameras will be used to photograph the license tags of some 400,000 vehicles so researchers can analyze freeway travel and predict future air-pollution levels and highway needs. The 43 cameras will photograph and track every car that passes on stretches of U.S. 74, and Interstates 77 and 85 during a 12-hour period on Tuesday. ... North Carolina highway officials say the photos will be destroyed within 90 days to protect the drivers. [Suuure they will - SCH]

Steve Holzworth, Senior Systems Developer sch@unx.sas.com  
SAS Institute - Open Systems R&D VMS/MAC/UNIX Cary, N.C.

[Interesting possibility if the numbers and letters can be read, but the state identification cannot -- in which case Steve in NC might get a ticket based on someone's Alaska licence plate. PGN]

---

## **⚡ Hacked caller ID?**

Andrew Hilborne <andrew.hilborne@uk.xo.com>  
*09 Aug 2001 18:09:52 +0100*

Two-and-a-half years ago I received an unexpected telephone call at about 2230 on my British Telecom phone. The caller was adamant that I had called him at about 2020 the same night, from my phone -- he had used

"1471" when he arrived home himself, to access the CLID of the last call to his number.

But I had been out of the house until 2200, and the house had been empty. It took some effort to persuade my unknown caller that I hadn't called him earlier that evening. So the following day I asked on the BT fault reporting line how this could have happened. I was told that this sort of thing happens quite often. I may well have been in trouble if a crime had been committed at the other house that night.

BT don't advertise this failure mode at all.

Andrew Hilborne

---

## **✶ Risks of letting MS not-so-Hotmail do your junk filtering...**

Michael Loftis <mloftis@wgops.com>

*Fri, 10 Aug 2001 09:01:38 -0700*

I see that Hotmail has junk/spam filter, I get a fair amount of SPAM in my hotmail account so I figure I'll give this a try. It doesn't block anything that is spam, in fact the only thing it did block in the "Low" setting was mailings from SPEAKEASY my ISP, even after I told it that I \*wanted\* those!

It's a good thing I noticed, they send bills via e-mail too.

I mean really! I got 3-4 pices of spam through the filter (even after

saying one of them was spam earlier) and 5-6 pieces of mail from Speakeasy went into the Junk folder with the filter, I turned it off.

The RISK is two-fold, blocking very obvious non-bulk mailings via a mechanism that isn't obvious, and then telling the user that they can ask that mechanism to be circumvented in special cases but not implementing it!!

Imagine if I had not looked into the Junk Mail folder? How much other legitimate e-mail would go into there, keep in mind this was the "Low" setting.

Michael Loftis

---

## **GPS-guide in car going nuts?**

Martin Schulze <joey@finlandia.infodrom.north.de>  
*Wed, 8 Aug 2001 18:09:33 +0200*

Modern cars may contain GPS systems to guide the driver to unknown destination locations he would otherwise have to use a map for.

We went out with three cars, of which two were sold with such a GPS system, ours wasn't, but we were driving in the city I know best. Both cars with GPS system didn't know that city well enough to reach the destination location without a map (or GPS system).

After lunch at a restaurant at a distant edge of the city we went back to

the house. Right after leaving the restaurant the three cars diverted, used different paths. Our car (w/o GPS) and one other car arrived at the house early. We were wondering where the third car had gone. Finally, some 10 minutes later, they arrived as well.

What was the reason? Too much trust and depending on modern computer thingies. The location was stored in the GPS system. In order to reuse the location it was stored by using letters, but unfortunately the display wasn't very wide. When storing the name of the city and some random string the system cut off some parts:

```
Wilhelmshaven Hotel
Wilhelmshaven House
Wilhelmshaven Restaurant
`-----'
Display
```

So when re-selecting the destination after lunch the driver had to make the choice which of the three similar looking locations is the proper one. He had selected the wrong one so the GPS system guided him to the hotel instead of the house.

This driver used the GPS system of a modern 'VW Passat', the other car was a 'Audi 100' which has a larger display for the GPS system, so the driver was guided to the correct address.

[Joey says "Please always Cc to me when replying to me on the lists."

That is always a good policy. PGN]

## ✦ The risks of not verifying e-mail addresses

Doug Winter <dwinter@businessseurope.com>

Thu, 9 Aug 2001 18:21:08 +0100

A colleague of mine recently received the following e-mail, apropos nothing:

```
> Date: Wed, 8 Aug 2001 16:41:07 +0530
> From: HDFC Bank Support <Support@hdfcbank.com>
> To: [name elided] <[address elided]>
> Subject: " Welcome to HDFC Bank.  "
>
> This is an auto-generated mail. Please do not reply to it.
> Dear Customer,
> Thank you for opening an account with us.
> We have received your account opening form and opened an
account as
> per the details mentioned below.
> You can now access all your accounts from any of our branches
across
> the country. To give you quick access to all your accounts
with us, we
> have generated a Customer Identification Number (Customer ID
No.). All
> your accounts are linked to this number, and you only need to
quote
> this number to our Personal Bankers or Tellers for any help you
> may require.
> Your Customer ID No. is [number elided].
> The Account details are:
> Account Number: [number elided]
> Primary Account Holder: [name elided]
> The Welcome Letter is being sent to you separately by mail.
[snip]
```

They sent a real account name, account number and customer ID to a complete stranger on the basis of a new user's registration information, without

first validating it in any way. The user in this case had / almost/ got his email address right - only the Top Level Domain was incorrect.

On informing the bank of their error they claimed "The information we send across to across e mail is limited hence the possibility of misuse is not possible".

The risks are obvious.

Doug Winter, CTO, Business Europe, 3 Waterhouse Square, Holborn Bars,  
142 Holborn, London EC1N 2NX +44 (0)20 7961 0341  
dwinter@businessseurope.com

---

## **✦ Re: Mixing advertising and credit-card activation (Green, [RISKS-21.57](#))**

Sam Garst <samgarst@netaxs.com>  
*Tue, 07 Aug 2001 14:30:12 -0400*

In [RISKS-21.57](#) Bob Green <rgreen@etnus.com> discussed a credit-card authorization process that raised some risks. I, too, was confused by a recent credit card activation; with an couple of novel (and risky) twists:

My credit card had been compromised. Kudos to the credit card agency, as they called me to confirm a suspicious (and fraudulent) charge. I dutifully called to activate my new card when it arrived. I have CallerID blocked, and I was curious to know how this might be handled. It wasn't, I sailed on

through the authorization process. Do they have the means to  
override  
CallerID blocking? Or, are they not validating the originating  
phone number  
as my home? I promise to call from my office next time, and  
report back.

Just as Bob Green mentioned, I was subjected to a rather long  
and tedious ad  
before the authorization process was complete. Ironically, the  
ad was for  
one of those credit reporting services, that will send you a  
consolidated  
report from all credit agencies, and alert you whenever someone  
makes a  
credit check. Well, I hope it was ironic and not targeted  
advertising for  
fraud victims.

Finally, the prompt at the end of the ad were deeply confusing,  
just as Bob  
Green noted. But wait, the confirmation prompt was reversed: "Do  
you want to  
buy this service?" <NO> "Are you sure you don't want to buy this  
service?"  
<YE...uh, wait, what was the question?>

Sam Garst <samgarst@acm.org>

---

**[Re: Mixing advertising and credit-card activation \(Green, RISKS-21.57\)](#)**

Joel Garry <joel-garry@home.com>  
*Tue, 07 Aug 2001 23:27:33 -0700*

>From Pacific Bell web page about caller id  
[http://www.pacbell.com/Products\\_Services/Residential/  
ProdInfo\\_1/1,1973,10-3-,00.html](http://www.pacbell.com/Products_Services/Residential/ProdInfo_1/1,1973,10-3-,00.html)

Complete Blocking prevents the transmission of your phone number on all calls you make, except 911 and national 800, 888, and 877 number calls.

The risk must be that adhesion contracts (with terms you are stuck with) may define a phrase like "Complete Blocking" with caveats that may unexpectedly negate the phrase. Of course, they are the phone company, they don't have to adhere to any reasonable man or reasonable computer standard.

A few days ago, I noticed my business line was in use. Since I wasn't using it, I picked it up and heard telephone technicians talking about line loops and how the "ants were biting the hell out of my arm." So I drove over to where they were installing DSL in the street and told a very surprised tech that if he didn't get off my line, I would make sure his supervisor would bite his ass a lot harder than those ants!

Joel Garry, Oracle and Unix Guy <http://www.garry.to>

---

## **★ REVIEW: "The Internet Security Guidebook", Juanita Ellis/ Timothy Speed**

Rob Slade <rslade@sprint.ca>  
*Mon, 13 Aug 2001 09:38:30 -0800*

BKISGFPD.RVW 20010605

"The Internet Security Guidebook", Juanita Ellis/Timothy Speed,  
2001,

0-12-237471-1, U\$44.95

%A Juanita Ellis

%A Timothy Speed tim.speed@home.com

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

%D 2001

%G 0-12-237471-1

%I Academic Press

%O U\$44.95 619-231-0926 800-321-5068 fax: 619-699-6380

%P 320 p.

%T "The Internet Security Guidebook: From Planning to Deployment"

The introduction outlines some of the basic types of attacks that can happen over the Internet, and seems to concentrate on attacks against machines, rather than people or companies. This emphasis on the technical is odd, since the material provides very few technical details, but does contain more than a little error and confusion. The text of the book doesn't mention a specific target audience, although the jacket notes seem to promote the work to CEOs and other senior executives. Which is odd: the writing level seems more appropriate to the home user.

Chapter one is an overview of security planning. Most of the important parts of preparation are included, but the chapter structure and even the figures are very confusing. There are many gaps in the discussion of security reviews, and a number of odd and apparently misplaced items have been inserted. Encryption is covered simplistically, and the lack of depth in the material becomes a problem in the chapter on network security. After twelve pages that \*don't\* explain the Internet and OSI (Open Systems Interconnection) models of networking, the text attempts to deal

with a number of Internet security tools, most of which rely on encryption and key exchange. There are frequent errors and the sections sometimes even provide contradictory and nonsensical explanations, such as the statement that "unencoded" means both "not encrypted" and "not as plain text." The basic outline of firewalls is better than is provided in most general guides, although the description of circuit-level gateways keeps referring to "stateful inspection" without ever explaining what that is. The long evaluation section is, unfortunately, the usual for this type of book: it does provide most of the right questions to ask, but doesn't give the novice reader much help in analyzing the answers. Authentication is a very important topic in security, and it is too bad that the material on this subject is so confused, and confusing. I find it very difficult to reconcile the statement that there are "very few examples" of biometrics with the existence of a great many fingerprint, palm geometry, iris, voiceprint, and even face readers. The depiction of Kerberos is wrong in some basic aspects, does not address the fundamental problems with the Microsoft version, and does not relate in any way to the very closely associated topic of single sign-on that immediately follows.

The discussion of PKI (Public Key Infrastructure) does do well in covering the "build or buy" debate for a certificate authority. Directory issues are not handled particularly well, and there are other errors. (Excuse me? The

Internet didn't exist before the mid- 1980s?) The chapter on messaging security is a real grab bag of topics, none of which, with the possible exception of acceptable use, are covered in sufficient depth. (Viruses and trojans get lumped into this chapter, and the commentary is quite sloppy.) The basic outline of risk analysis, including threat, impact, and probability, is good, but the supporting material is not quite standard, and probably not very helpful to the target audience. The chapter also fails to point out the full scope of such an appraisal, as well as the importance of looking at the aggregate risk. On the other hand, the review of policy and procedures hardly seems to address policy creation at all. This is another miscellaneous compendium of vulnerabilities, diving into specifics and missing the bigger picture. The material on incident response is generic, but does point out the foundational concepts. There is little detail, and the text does concentrate on dealing with events by severity, rather than by type. The book closes off with an ordinary presentation on project planning.

I would be the first to admit that security can be a dry topic, and a little humour can help to spice up the text. However, I am willing to make an exception in the case of this book. The jokes added to the text do nothing to improve it. They are intrusive, distracting, and do not, in any way, help the reader to understand the topics under discussion. Indeed, the attempts at comedy generally sidetrack the reader from the central issues of

the work, and simply confuse any issue under discussion.

If this text is aimed at executive management, it definitely needs to be tightened up and reorganized to eliminate duplicated material and ensure the structure and arguments are easier to follow. Many points raised throughout the work are important, but a number of vital issues are not addressed, and the patchwork of writing level and quality of information probably means that this is unsuitable as an only introduction to security. The Internet, in fact, is not really a major concern in this book, although it does get mentioned from time to time. I would have difficulty in suggesting a group that would benefit from this book, although it might serve as an adjunct text to the security planning process, if ideas were being culled from multiple sources.

copyright Robert M. Slade, 2001 BKISGFPD.RVW 20010605  
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>

---

## **✶ Dependability and "Open Source" development**

Cliff Jones <cliff.jones@ncl.ac.uk>

*Wed, 15 Aug 2001 13:39:14 +0100*

WORKSHOP ON OPEN SOURCE SOFTWARE DEVELOPMENT  
NEWCASTLE, 25-26 FEBRUARY 2002

Organised by the Dependability of Computer-Based Systems ([www.dirc.org.uk](http://www.dirc.org.uk))

Interdisciplinary Research Collaboration, the focus is on dependability and open source software development. Short abstracts

due by 2 Nov 2001, papers later. For further details, see:

[http://www.dirc.org.uk/events/ossdw\\_ncl.html](http://www.dirc.org.uk/events/ossdw_ncl.html)

and contact Dr. C. Gacek <[cristina.gacek@ncl.ac.uk](mailto:cristina.gacek@ncl.ac.uk)>.

---

## ✶ CFP2002: Call for Proposals

"Lance J. Hoffman" <[hoffman@seas.gwu.edu](mailto:hoffman@seas.gwu.edu)>

Wed, 01 Aug 2001 19:48:44 -0400

[CFP has been an extraordinarily valuable conference, bringing together

a very diverse group. Strongly recommended. Proposals due 15 Oct 2001.

(This CFP CFP has been abridged for RISKS.) PGN]

CFP2002: The Twelfth Conference on Computers, Freedom & Privacy  
Cathedral Hill Hotel, San Francisco, California, USA

16-19 April 2002

<http://www.cfp2002.org>

Lance J. Hoffman, The George Washington University, Washington DC 20052:

Professor, Dept. of Computer Science [www.cs.seas.gwu.edu](http://www.cs.seas.gwu.edu) (202) 994-4955

and Cyberspace Policy Institute (202) 994-5513 [www.cpi.seas.gwu.edu](http://www.cpi.seas.gwu.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 21: Issue 61**

**Friday 17 August 2001**

## Contents

- [Censorship in action: why I don't publish my HDCP results](#)  
[Niels Ferguson](#)
- [Florida relies on students, not experts](#)  
[Adam Shostack](#)
- [PDAs increasingly vulnerable to hackers](#)  
[Monty Solomon](#)
- [Welland Canal Bridge runs into ship](#)  
[Chris Smith](#)
- [U.S. Web sites fall short of global privacy standards](#)  
[NewsScan](#)
- [DejaGoogle rides again](#)  
[Dave Weingart](#)
- [Risks to lose sleep over](#)  
[Mike Knell](#)
- [Re: AT&T Worldnet exposes all user passwords](#)  
[Dylan Northrup](#)  
[Mike Tuffs](#)
- [Telephone "\\*" codes](#)  
[Alan Miller](#)
- [Info on RISKS \(comp.risks\)](#)

## ✂️ **Censorship in action: why I don't publish my HDCP results**

Niels Ferguson <niels@ferguson.net>

*Fri, 17 Aug 2001 22:49:48 +0200*

[Copyright Niels Ferguson. Published with permission of the author. PGN]

Censorship in action: why I don't publish my HDCP results  
Niels Ferguson, 15 Aug 2001

### Summary

I have written a paper detailing security weaknesses in the HDCP content protection system. I have decided to censor myself and not publish this paper for fear of prosecution and/or liability under the US DMCA law.

### Introduction

My name is Niels Ferguson. I'm a professional cryptographer. My job is to design, analyse, and attack cryptographic security systems, a bit like a digital locksmith. I work to make computer systems and the Internet more secure. You would think that people would be in favour of that, right?

Computer security and cryptography are hard. It is easy to make mistakes, and one mistake is all it takes to create a weakness. You learn from your mistakes, but there are too many mistakes to make them all yourself. That's why we publish. We share our knowledge with others, so that they don't have

to repeat the same mistake. Take a look at  
<<http://www.macfergus.com/niels/dmca/index.html../pubs/publist.html>>my  
publications. You will see a mixture of new designs, analyses,  
and attacks.  
This is how we learn and how we improve the state of the art in  
computer  
security.

## HDCP

Recently I found the documentation of the  
<<http://www.digital-cp.com>>High-bandwidth Digital Content  
Protection (HDCP)  
system on the Internet. HDCP is a cryptographic system developed  
by Intel  
that encrypts video on the DVI bus. The DVI bus is used to  
connect digital  
video cameras and DVD players with digital TVs, etc. The aim of  
HDCP is to  
prevent illegal copying of video contents by encrypting the  
signal.

HDCP is fatally flawed. My results show that an experienced IT  
person can  
recover the HDCP master key in about 2 weeks using four  
computers and 50  
HDCP displays. Once you know the master key, you can decrypt any  
movie,  
impersonate any HDCP device, and even create new HDCP devices  
that will  
work with the 'official' ones. This is really, really bad news  
for a  
security system. If this master key is ever published, HDCP will  
provide no  
protection whatsoever. The flaws in HDCP are not hard to find.  
As I like to  
say: "I was just reading it and it broke."

What do you do when you find a result like this? First, you have  
to write  
it down and explain it. Then you publish your paper so that the  
mistakes

can be fixed, and others can learn from it. That is how all science works.

I wrote a paper on HDCP, but I cannot publish it.

DMCA

There is a US law called the Digital Millennium Copyright Act (DMCA), that makes it illegal to distribute "circumvention technology", such as systems that break copyright protection schemes. HDCP is used to protect copyrights. There are lawyers who claim that a scientific paper like mine is a circumvention technology within the meaning of the DMCA, because it explains the weaknesses of a system. I have been advised by a US lawyer who works in this field that if I publish my paper, I might very well be prosecuted and/or sued under US law.

This is outrageous.

The risk to me

I travel to the US regularly, both for professional and for personal reasons. I simply cannot afford to be sued or prosecuted in the US. I would go bankrupt just paying for my lawyers.

I want to make it quite clear that Intel, who developed the HDCP system, has not threatened me in any way. But the threat does not come only from Intel. The US Department of Justice could prosecute me. Any other affected party, such as a movie studio whose films are protected with HDCP, could sue me under the DMCA. That is a risk I cannot afford to take.

The simple alternative would be to never travel to the US again. This would

harm me significantly, both professionally and personally. It would lock me out of many conferences in my field, and keep me away from family and friends.

It all sounds a bit too far-fetched, right? Who would sue over the publication of an article? Well, there are very good reasons to believe that I risk a lawsuit if I publish my paper. A team of researchers led by Professor Edward Felten was recently threatened with a DMCA-based lawsuit if they published their own scientific article. The resulting court case is still pending.

#### Freedom of speech

We have this little principle called the freedom of speech. It is codified in the <http://www.hrweb.org/legal/udhr.html> Universal Declaration of Human Rights, the <http://www.law.emory.edu/FEDERAL/usconst.html> US Constitution, and Dutch law. The whole point of freedom of speech is to allow the free circulation of ideas and to let the truth be heard. There can be no doubt that my paper is protected by the free speech rights.

The DMCA imposes a serious restriction on the freedom of speech. The DMCA makes it illegal to talk about certain security systems. The equivalent law for non-digital protection systems would make it illegal to warn people about a cheap and very weak door lock being installed on their houses because criminals could also use that same information.

In western society we restrict the freedom of speech only for very serious

reasons, and after careful consideration. For example, it is illegal to shout "fire" in a crowded theatre, or to ask someone to commit a murder.

The DMCA restricts the freedom of speech because the movie industry is afraid of losing money. Below I will argue that the DMCA does not achieve that goal, but that aside: do we really want to sell our freedom of speech for money?

The DMCA is a scary development. Next time that commercial interests clash with the freedom of speech, the industry will point to the DMCA and claim they need equivalent protection. They might outlaw the publication of a report detailing bad safety features in a car, or of flaws found in a particular brand of tires. After all, those publications harm industry too. Where will it stop?

## Jurisdiction

The DMCA is a US law. I am a citizen of the Netherlands, and I live and work in Amsterdam in the Netherlands. Why do I care about the DMCA at all?

The USA is apt to apply its own laws way beyond its own borders. Dmitry Sklyarov, a Russian programmer, was arrested last month in the US. He is charged with violating the DMCA while performing his work in Russia as an employee for a Russian firm. As far as we know, what he did was perfectly legal in Russia, and in most other countries in the world. He is now out on bail, but cannot leave northern California until further notice.

Where does this lead to? What if countries start applying their own laws to the things people do in other countries? Will you be arrested next time you go abroad? Do you really want to take that holiday in China if you have more than one child? Are you sure that Germany allows you to have those links to political pamphlets on your web site? This type of extraterritorial application of national law violates a basic human right, because you cannot possibly know which laws apply to you. Imagine living in a country where the laws are kept secret, and you never know whether you are violating a law.

Suppose a US citizen works for a firearms manufacturer in the US, making guns. One of those guns turns up here in Amsterdam and is used to commit a crime. This person takes a holiday over here in Europe, and is arrested for violating the Dutch firearms laws because he helped manufacture the gun in the US. That is what happened to Dmitry. Is that fair? Is that how we want to run this world?

The principle of applying national laws to anybody that publishes anything anywhere in the world is terrifying. If we allow this principle to be used, we will never be free again. You will get a choice. You can decide to never leave your country for any reason whatsoever. This means you might not even be able to attend a wedding or funeral of a loved one. Alternatively, you can restrict all your statements to satisfy the laws of all the countries you could conceivably travel to. You might as well not say anything,

because it is very hard to find something that is legal in all jurisdictions. We either lose our right to travel, or our right to speak and be heard. Which fundamental human right do you want to give up today?

DMCA does not work

The DMCA is a fundamentally flawed law. It is ineffective, and actually harmful to the interests it tries to protect. It stops me publishing my paper now, but someday, someone, somewhere will duplicate my results. This person might decide to just publish the HDCP master key on the Internet. Instead of fixing HDCP now before it is deployed on a large scale, the industry will be confronted with all the expense of building HDCP into every device, only to have it rendered useless. The DMCA ends up costing the industry money. No points for guessing who ends up paying for it in the end.

In the long run, the DMCA will make it much easier to create illegal copies. Why? If we cannot do research in this area, we will never develop good copyright protection schemes. We will be stuck with flawed systems like HDCP, to the delight of the criminals.

The DMCA has been called the Snake Oil Protection Act. When a manufacturer makes a defective product, you expect them to fix it. Not in this case. The DMCA protects the manufacturer of a defective product by making it illegal to show that the product is defective. Who came up with this idea?

## Copyright law

Copyright law is a careful balance between the rights of the author and the public interest. The author gets a limited-time exclusive right to reproduce his work. The public gets free use of the work once the copyright expires. Furthermore, the public gets certain "fair use" rights. These include the right to use short quotes from the work in a review, for example, and the right to create a parody. If you buy a copy of a copyrighted work, you also have the right to make an extra copy for your own use. A student can make a copy of a page in his textbook to mark it up while he studies.

In a sneaky way the DMCA eliminates all these "fair use" rights of the public. As long as the work is protected using copyright protection technology, none of the "fair use" rights can be exercised, because it is illegal to create or own the tool with which you can exercise your fair use rights. Copyright expires, but the DMCA ensures that even when it does, the work still does not enter the public domain. The US supreme court has held that the "fair use" rights are exactly the safety valve that prevent the copyright law from violating free speech rights. This might be another reason why the DMCA is unconstitutional.

In Dmitry's case, he wrote software that decoded encrypted digital books. His software has many uses. Many digital books only allow the book to be viewed on the screen. If you are blind and want to read the book on your

braille display you have to use something like Dmitry's software. This is perfectly legal under the "fair use" rules of copyright law, but the DMCA forbids it thereby prohibiting blind people from accessing such books.

Why this mess?

Why did the movie industry campaign for the DMCA if it doesn't work? The movie and record industry have a history of claiming that new technologies will bankrupt them. When video recorders were first introduced, they swore that they would go bankrupt if people could record movies. Now they make a lot of money selling video tapes. Now they swear that they will go bankrupt if we do not restrict the freedom of speech and the public's fair use rights. Why should we believe them this time around?

The DMCA exists because the movie and record industry lobbied heavily for it. It is a very one-sided law that clearly has not been thought through properly. The industry has managed to eliminate the careful balance of the copyright law and replace it with a law that effectively gives them an unlimited monopoly on copyrighted works. Could it just be that this is the real motive behind their lobby?

Can we fix the DMCA?

Sure. That wouldn't even be very difficult. Making and selling unauthorised copies of copyrighted works is already illegal in most jurisdictions. We could change the copyright law to impose stiffer penalties if the copyright

violation involves breaking a copyright protection scheme. A bit like the difference between trespassing and breaking and entering. A law like this would achieve exactly what we want: it would restrict illegal copying of copyrighted works. It would not restrict the freedom of speech, or do away with our fair use rights.

More information

You can find lots more information about the DMCA and the cases of Professor Felten and Dmitry Sklyarov on the <<http://www.eff.org>>EFF web site.

My <[http://www.macfergus.com/niels/dmca/index.htmlfelten\\_declaration.html](http://www.macfergus.com/niels/dmca/index.htmlfelten_declaration.html)> declaration in the Felten court case.

Copyright 2001 by Niels Ferguson, last update 2001-08-16, comments to

<<mailto:niels@ferguson.net>>niels@ferguson.net  
<<http://www.macfergus.com/niels/dmca/index.html../index.html>>  
[home page]

---

## ✶ Florida relies on students, not experts

Adam Shostack <[adam@zeroknowledge.com](mailto:adam@zeroknowledge.com)>  
*Fri, 17 Aug 2001 13:26:15 -0400*

> FORT LAUDERDALE, Fla. (AP) - Broward County officials considering  
> the \$20 million purchase of a touchscreen voting system want  
> students to try to tamper with the computers during a mock election.  
>  
> "One of the biggest concerns raised is whether there is the

> potential for computer abuse, and we really need to see how  
> foolproof or tamperproof this equipment is," county commission  
> Chairman John Rodstrom said. "If there is a problem, it will  
happen  
> now or later. And some of these kids are pretty smart."  
> <http://ap.tbo.com/ap/florida/MGAJ6W8YGQC.html>

The risks are legion, and well documented. It's too bad that Florida officials are relying on students to reproduce them, but hey, one of them may learn the value of reading the literature, instead of re-inventing it.

[And if someone with very little experience can demonstrate the lack of security, \*that\* might impress some of the folks who are either supremely gullible or counting on opportunities for fraud. But please remember that some of the most insidious riskful vulnerabilities are those that can be exploited by insiders in the development and maintenance process. Once again, recognize that all of the touch-screen systems today have absolutely no independent voter-verified audit record such as a printed ballot image that can be stored in ballot boxes guarded at least as well as paper ballots are today -- whether punched-card or optically scanned. Thus, there is no reasonable guarantee in touch-screen systems that your ballot as cast is actually equivalent to the ballot that is counted. This could be remedied relatively easily, as recommended in Rebecca Mercuri's PhD thesis <<http://www.notablessoftware.com/evote.html>>. PGN]

---

## ⚡ PDAs increasingly vulnerable to hackers

Monty Solomon <monty@roscom.com>

*Fri, 17 Aug 2001 02:50:22 -0400*

Handheld computers are increasingly vulnerable to hacker attacks and should not be trusted to store "any critical or confidential information," security experts warned Thursday. [Reuters, 16 Aug 2001]

<http://news.cnet.com/news/0-1006-200-6894699.html>

---

## ⚡ Welland Canal Bridge runs into ship

Chris Smith <smith@interlog.com>

*Fri, 17 Aug 2001 13:01:17 EDT*

[Three parts, sent separately, merged into one item. PGN]

1. Sent 13 Aug 2001

The following two news reports from the Canadian Broadcasting Corporation cover a Saturday evening accident in the Welland Canal (southern Ontario, Canada, near the border with Buffalo, NY) when a lift bridge was lowered too soon, shearing off the top of the wheelhouse of a 700 ft bulk freighter. Damage to the out-of-control freighter followed, first in collision with the canal, and then with a fire breaking out on board. The fire flared up again briefly Monday morning.

At least one news report stated that the bridge is under remote

control,  
with bridge cameras monitored from the remote control location.  
For now, the  
clear risk is not having a working fallback to deal with  
situations that are  
never supposed to happen. We await news of what went wrong (we  
hope  
something did actually go wrong!) that gave rise to this  
accident.

[http://cbc.ca/cgi-bin/templates/view.cgi?/news/2001/08/12/  
shipfire\\_010812](http://cbc.ca/cgi-bin/templates/view.cgi?/news/2001/08/12/shipfire_010812)

[http://cbc.ca/cgi-bin/templates/view.cgi?/news/2001/08/13/  
shipfire\\_010813](http://cbc.ca/cgi-bin/templates/view.cgi?/news/2001/08/13/shipfire_010813)

Here is a good location to read further details and watch for  
continuing  
details. This page is maintained by a regular canal and ship  
watcher in the  
area:

<http://www.wellandcanal.ca/transit/2001/august/windocstory.htm>

2. Sent 16 Aug 2001

Just to make me look silly, I'm certain, the report is now that  
the bridge  
is run directly from a command cabin on the lift section itself.  
(I checked  
the CBC video stream, and they did explicitly say the bridge was  
under  
remote control.)

This makes a lot more sense, especially from the point of view  
of avoiding  
accidents. Which leaves us with an open RISKS question to be  
checked later  
when it is known what caused this collision.

3. Sent 17 Aug 2001

As the referenced newspaper article makes clear, the Welland  
Canal bridge

that collided with the freighter "Windoc" was \*not\* a remotely-operated bridge:

<http://www.scstandard.com/news/010814/5106699.html>

This contradicts -- authoritatively -- the statement earlier in a Canadian Broadcasting Corporation report that the bridge was remotely controlled.

Only one of eight lift-bridges across the canal is remotely controlled. The rest are staffed 24 hours a day during the shipping season.

The article gives a good description of the ship-bridge passage protocol.

Chris Smith <smith@interlog.com>

---

## **✶ U.S. Web sites fall short of global privacy standards**

"NewsScan" <newsscan@newsscan.com>

*Fri, 17 Aug 2001 08:52:25 -0700*

A survey of 75 U.S. corporate Web sites found that none were in compliance with a set of international privacy guidelines developed by the U.S. and the European Union last year. The guidelines require companies to: notify consumers how their personal data is used; use the information only for its stated purpose; allow consumers to examine and correct data collected about them; give consumers an option to forbid sharing that data for marketing purposes; store the data in a secure manner; and provide

recourse for consumers whose privacy has been violated. The survey, conducted by Andersen, found that travel and leisure companies scored the best on notice and security provisions, while financial services firms were most likely to offer adequate choice. U.S. companies must make progress on revamping their Web privacy standards or "Disruption to the conduct of business is a real risk," says Andersen principal Kerry Shackelford.

[Reuters 16 Aug 2001; NewsScan Daily, 17 August 2001]

<<http://news.excite.com/news/r/010816/11/net-tech-privacy-dc>>

---

## ⚡ DeJaGoogle rides again

Dave Weingart <dave.weingart@us.randstad.com>

*Fri, 17 Aug 2001 13:30:19 -0400*

I recently had to look for a message in rec.arts.sf.fandom, one of the Usenet groups I follow and popped onto <http://groups.google.com> (Google having taken over Deja's Usenet archives). Knowing the thread title and the approximate date, I entered those into Google's advanced group search. Bingo, one result returned, with a notice that read:

"In order to show you the most relevant results, we have omitted some entries very similar to the 1 already displayed. If you like, you can repeat the search with the omitted results included."

Whoops. The omitted entries were *\*all\** the other entries in the rest of the

thread -- clicking on the link they provide shows all the other messages. I

leave the risks of this behavior as an exercise for the reader.

Dave Weingart, Randstad North America dave.weingart@us.randstad.com

1-516-682-1470

---

## ⚡ Risks to lose sleep over

Mike Knell <mpk@lspace.org>

*Sat, 11 Aug 2001 10:01:33 +0100*

While staying in a German youth hostel a couple of weeks ago, I was woken up at midnight by someone telling me I hadn't paid to stay that night, so would have to pay them DEM33 or leave. Ungh, gnurgh, I said (having been freshly woken up), no, I've definitely paid in advance for two nights. This is the second night. No, they said, you've only paid for one.

Okay, okay. Look, I've got a receipt. Can I come downstairs and sort this out? Sure thing, they said. Better be down in five minutes at the most.

So I put some clothes on, found the receipt in my wallet and presented it at the front desk. Sure enough, it was a receipt for 2\*DEM33 == DEM66. Two nights, all paid. But no, they said. Look, the departure date printed on your receipt shows you've only paid for one night, and the computer agrees, so you'll have to pay us DEM33 for tonight or leave. By now I was beginning to wonder whether I was hallucinating. My receipt for two nights wasn't

being accepted as such? Why not? At about this point I stopped speaking German and switched to English, because arguing in a foreign language when you've been awake for two minutes and you're starting to doubt your sanity anyway is tricky.

After a bit more arguing of the "I've paid!" "No, you haven't!" sort, and a lot more fiddling about with the registration computer, the problem was solved. Yes, I'd paid two nights at DEM33 each. But this had been recorded in the booking system as 2 persons for one night, not one person for two nights, so I'd been flagged as having departed. This also explains the discrepancy in the departure date on the receipt. Since everything was now In Order, I was graciously permitted to return to my dorm and go back to sleep.

The RISKS here are obvious -- the computer's not always right when it's been given the wrong information in the first place. This was, however, the first time I've encountered anyone not believing the evidence of their own eyes -- my receipt for two paid nights and my keycard with the correct departure date written on it -- because the computer didn't agree with it. I'd also mention the RISKS of waking me up in the middle of the night just to annoy me like this, but they're pretty obvious too.

Mike <mpk@lspace.org>

## ✶ Re: AT&T Worldnet exposes all user passwords ([RISKS-21.57](#))

Dylan Northrup <docx@io.com>

Tue, 7 Aug 2001 15:35:56 -0500 (CDT)

An infinite number of monkeys in the guise of a RISKS contributor wrote:

```
:=Then she asked for my e-mail password.  When I refused she
:=informed me my password is not a secret, and that *all
passwords* connected
:=to my Worldnet account (a Worldnet account can have up to 6 e-
mail accounts)
:=are *visible* on her screen.
```

This is not surprising. When working for another major ISP, the database for their users also had passwords available for each customer and were used by customer service as well as system administrators to help diagnose specific problems with customers. When working with a problem that affects a specific customer, sometimes the best way to reproduce it from the other end is to use the service as the customer.

That the CS representative asked for your password is unique or at least questionable (our user base was instructed to never give that information over the phone and that CS reps would be able to access that information if necessary).

Dylan Northrup <\*> docx@io.com <\*> <http://www.io.com/~docx/>

---

## ✶ Re: AT&T Worldnet exposes all user passwords (Smith, [RISKS-](#)

## [21.57\)](#)

"Tuffs, Mike" <mike\_tuffs@mentorg.com>

Wed, 8 Aug 2001 09:47:55 -0700

WRT the comments in this posting about blocking caller-id when used for credit-card authorisation purposes, I recently called a credit-card company to authorize my new card, using a blocked caller-id. The system was able to identify me without anything other than my card number, due to caller-id.

When I asked how they were able to do this, as the id was blocked, they informed me that their equipment simply ignored the blocked bit in the id string. I assume this is possible for anyone?

Mike Tuffs, Mentor Graphics Corp (503) 685 0736

mike\_tuffs@mentor.com

---

## **⚡ Telephone "\*" codes (Re: Burstein, [RISKS-21.59](#))**

Alan Miller <ajm@enteract.com>

Tue, 14 Aug 2001 12:36:12 -0500

Danny Burstein writes on CNID/Caller ID:

>The former, which is what is used by (the vast majority of) homes and

>"regular" (non "800") business lines, can be blocked by the caller on

>either a permanent per-line basis, or as a choice per-call.

(Usually by

>prepending a special code, generally "\*70", before dialing out).

Actually, "\*70" is almost always the code to toggle call waiting

notification, primarily used so incoming calls won't cause a beep on the line while a data call is in progress.

"\*67" is the most commonly used code to toggle outgoing caller ID information. This was discussed fairly heavily in RISKS or the Telecom Digest (or both) when caller ID first became available, since for customers with per-line blocking it's the code to `_enable_` caller ID for the following call, and there's no way to find out whether caller ID is enabled for a line or call.

In some areas, "\*69" is used for "last number callback," which calls the number that originated the previous call (answered or not, I believe).

I believe that this service has a range of options and is handled differently by different LECs.



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 21: Issue 62**

**Saturday 25 August 2001**

## Contents

- [Oklahoma whistleblower asked to accept felony conviction](#)  
[Deborah Weisman](#)
- [Follow-up on Oklahoma whistleblower](#)  
[PGN](#)
- [Wireless security vulnerabilities](#)  
[PGN](#)
- [AirSnort!](#)  
[PGN](#)
- [Kaiser Permanente](#)  
[identity withheld by request](#)
- [Air Force officer mails confidential information to all cadets](#)  
[Jim Griffith](#)
- [Re: Avoiding prosecution of the DMCA](#)  
[David Petrou](#)  
[Fred Cohen](#)
- [Re: Why I don't publish my HDCP results](#)  
[Bill Weitze](#)  
[David Gillett](#)
- [Re: rot13](#)  
[Mike Perry](#)

- [Hack the vote? Not in Broward County!](#)  
[James Paul](#)
  - [Re: Runway incursions](#)  
[Bill Hopkins](#)
  - [Code Red 9? Code Crimson](#)  
[Alistair McDonald](#)
  - [AT&T - the computer MUST be right!](#)  
[Sharon Mech](#)
  - [Re: DejaGoogle rides again](#)  
[Geoffrey Leeming](#)
  - [Re: Risks of automated junk/spam filters](#)  
[AlphaLau](#)
  - [Yet another MS Hotmail risk](#)  
[Kimmo](#)
  - [REVIEW: "SSL and TLS", Eric Rescorla](#)  
[Rob Slade](#)
  - [Dependable Systems and Networks DSN-2002 Call for Contributions](#)  
[Anup Ghosh](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

## 🚨 Oklahoma whistleblower asked to accept felony conviction

Deborah Weisman <dvorah@agri.huji.ac.il>

Wed, 22 Aug 2001 10:40:06 +0300

A Federal prosecutor has asked Brian West, a 24-year old sales and support employee of an Oklahoma ISP "to accept a felony conviction and 5 years probation" for notifying the editor-in-chief of his local newspaper \*Poteau Daily News\* that they had failed to set up password security for their Web site: no authentication, anyone could edit the site using Microsoft FrontPage. Following their phone conversation, the EIC gave a

tape of the conversation to the Poteau Police Department, who invoked the FBI.

[<http://www.macintouch.com/newsrecent.shtml>; PGN-ed]

Computer Center Faculty of Agriculture Hebrew University of Jerusalem

P.O.B. 12 Rehovot 76100 ISRAEL 972-8-9489232 dvorah@agri.huji.ac.il

[Also noted by Ron LaPedis at

<http://www.linuxfreak.org/post.php/08/17/2001/134.html>. PGN]

---

## **Follow-up on Oklahoma whistleblower**

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

*Sat, 25 Aug 2001 10:12:13 PDT*

Sheldon Sperling <Sheldon.Sperling@usdoj.gov>, the U.S. Attorney in the

Brian K. West case, has responded to various e-mail protests on his handling

of the case. He claims that West was not arrested and has not been charged.

However, an investigation is pending, to determine whether West "intentionally accessed a computer without authorization or exceeded

authorized access (to access a computer with authorization and to use such

access to obtain or alter information in the computer that the accesser is

not entitled so to obtain or alter), (2) whether the employee thereby

obtained information from a protected computer (a computer which is used in

interstate or foreign commerce or communication), and (3)

whether the

conduct involved an interstate communication. 18 USC

1030." [The full statement from Sperling is included in a message from Declan McCullagh, which is accessible at <http://www.politechbot.com/> .]

I have noted in this space before that when there is no security in place, the alleged culprit cannot have exceeded authority when no authority is implied. As long-time RISKS readers will recall, this issue came up relating to the trial of Robert Tappan Morris: in 1988, the Internet worm never exceeded authority, because no authority was required to use the sendmail debug option, to use the .rhosts mechanism, to execute the finger daemon, or to read an unprotected encrypted password file. I wonder how if prosecutors will ever figure this out!

As long as we attempt to shoot the messenger and hide lame security behind overly broad laws, weak security will prevail, and whistleblowers will be much rarer than glassblowers. (For example, DMCA is among other things an attempt to outlaw whistleblowers.)

---

## **Wireless security vulnerabilities**

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

*Sun, 19 Aug 2001 13:16:18 PDT*

Sitting in the Morristown (N.J.) Memorial Hospital, AT&T Labs' Avi Rubin (a note from Avi on WEP insecurity is in [RISKS-21.57](#)) noticed that his laptop

wireless connection card was blinking, and then discovered that the hospital's wireless network was open to his laptop, using 802.11b (Wi-Fi) and automatically granting him access. [Source: As Wireless Networks Grow, So Do Security Fears, by John Schwartz Sunday Business Section of \*The New York Times\*, page 10, 19 Aug 2001 (National edition), PGN-ed; full article at

<http://www.nytimes.com/2001/08/19/technology/19WIRE.html>]

[Another case of \*not\* having to exceed authority because there was no security involved! Sloppy hospital? Insecurity by obscurity? PGN]

---

## **AirSnort!**

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

*Fri, 24 Aug 2001 11:52:33 -0700*

AirSnort, WEPCrack, and other programs available on the Internet make it easy to sniff sensitive data such as passwords that fly around 802.11b wireless Internet networks. A competing standard, Bluetooth, is not susceptible, although Bluetooth is considered "more vulnerable to spies than hard-wired networks." [Source: AP item, 24 Aug 2001, courtesy of Ken Nitz; PGN-ed]

The vulnerabilities have been noted here before, but now maybe there will be some incentives to do something about it? On the other hand, probably not, if our historical RISKS warnings are not observed,

as usual.

---

## **✶ Kaiser Permanente**

<identity withheld by request>

*Tue, 21 Aug 2001 19:23:53 -0700*

There's a self-service section on the Kaiser Permanente (an HMO) Web site at

<http://www.kaiserpermanente.org/> that allows you to notify them of a change

of address. In bold letters next to the submit button, it claims "Your

information is secure!". Sounds good. Checking View Source showed the form

was being submitted over SSL. Ok, let's submit the information. A few

minutes later an e-mail arrives. No encryption. Ouch -- it contains a

verbatim copy of the personal information I typed into the form. So much

for "Your information is secure!".

Why bother breaking SSL flows, when you can just watch the e-mail?

---

## **✶ Air Force officer mails confidential information to all cadets**

Jim Griffith <griffith@olagrande.net>

*Sat, 25 Aug 2001 14:48:44 -0500*

AP reports that an Air Force Academy officer accidentally sent confidential

information about some 40 cadets to all 4400 cadets at the

school. The mail in question contained details of past and pending disciplinary issues, including the identity of confidential informants in some cases. The information in question was reportedly protected by federal law, and officials subsequently ordered cadets to delete the letters.

<http://www0.mercurycenter.com/breaking/docs/044576.htm>

---

**⚡ Re: Avoiding prosecution of the DMCA (Ferguson, [RISKS-21.60](#))**

David Petrou <[dpetrou@cs.cmu.edu](mailto:dpetrou@cs.cmu.edu)>

*Sun, 19 Aug 2001 20:56:30 -0400*

Just staying out of the U.S. won't necessarily do the trick. The DoJ can obtain an arrest warrant based upon a criminal violation of the DMCA and seek extradition from a number of countries. If US law is violated and the country where the person is has an extradition agreement with the United States, the foreign government will cooperate in arresting the person and having that person delivered to the United States for prosecution.

---

**⚡ Re: Avoiding prosecution of the DMCA (Ferguson, [RISKS-21.60](#))**

Fred Cohen <[fc@all.net](mailto:fc@all.net)>

*Fri, 17 Aug 2001 15:47:51 -0700 (PDT)*

The DMCA has also had effects on my forensic analysis products. Because the current copyright law makes anything that is put into tangible form copyright unless made otherwise by the author (or by law), things like criminal records are copyright.

This means that if the criminal tries to protect their material - for example by hiding it using steganography, encrypting it, or by putting it on a computer with a password to prevent unauthorized access - then that work is protected by the DMCA (after all, the password on Windows systems is effective protection unless you try to circumvent it).

Because the primary purpose of most of my forensic analysis tools is to reveal things that are protected from revelation, and because the DMCA makes it illegal to distribute such a device, I have been forced (based on the recent arrests and other threats against authors of such things) to withdraw my forensic products from the market.

I should note that companies like Access Data who sell products that are explicitly designed for undoing encryption, etc. are almost certainly in violation of the DMCA. While the FBI might not arrest them now because they sell to the FBI (and other in law enforcement - as did I), this does not mean that the FBI cannot arrest them at any time and charge them with a felony. Indeed, sale to law enforcement is not legal, even though law enforcement can, on its own, build and use such tools.

The effects on research and education are even more interesting. For example, I am having a discussion with my university now about canceling courses on forensics and cryptanalysis because in these courses we teach people how to get around protection of this sort and may provide the capabilities to do so in so teaching. The DMCA has, I believe, made this illegal - and if you are teaching such a course next semester, you might think about the issues as well. On the research side, I don't work on research I cannot publish, so I am canceling the aspects of my research that go into these areas.

Fred Cohen  
fax:925-454-0171  
fc@all.net  
[www.unhca.com/](http://www.unhca.com/)  
<http://all.net/>  
tel:925-294-2087

Fred Cohen & Associates.....tel/  
The University of New Haven.....<http://>  
Sandia National Laboratories....

---

## **✶ Re: Why I don't publish my HDCP results (Ferguson, [RISKS-21.61](#))**

"Bill Weitze" <bweitze@california.com>  
*Fri, 17 Aug 2001 21:36:04 -0700*

Hmm, a blind person could sue the publisher under the Americans with Disabilities Act.

> Why did the movie industry campaign for the DMCA if it doesn't work? The  
> movie and record industry have a history of claiming that new

technologies  
> will bankrupt them.

They complain about paper books, too. In the September 18, 2000 issue of U.S.

News and World Report, p. 55, an article titled "The empire strikes back"

states the following:

A typical book, for example--the old-fashioned kind--finds its way to five

or six readers beyond the original purchaser, according to Laurence

Kirshbaum, CEO of Time Warner's trade-publishing arm. "One of the

attractions of electronic publishing," he says, is the ability to "cut down

on this pass-along."

I wrote to U.S. News as follows:

This "loaning", as its practitioners call it, is indeed most subversive.

There are even institutions, called "libraries", which carry on this sort

of thing in a wholesale fashion. This was started by a very dangerous

individual named Franklin; maybe Mr. Kirshbaum should sue him.

Bill Weitze, San Jose, CA

---

**✶ Re: Why I don't publish my HDCP results (Ferguson, [RISKS-21.61](#))**

David Gillett <dgillett@deepforest.org>

*Fri, 17 Aug 2001 16:38:04 -0700*

To my mind, one of the more dangerous aspects of DMCA is the

deliberate  
conflation and confusion of "copy protection" (use restriction  
mechanisms)  
with "copyright protection". Experience has already shown that  
the former  
are not an acceptable substitute for the latter, a lesson which  
DMCA  
attempts to unlearn by fiat.

---

## ⚡ Re: rot13 ([RISKS-21.58](#) and [.59](#))

"Mike Perry" <PERRYM@uk.ibm.com>  
*Tue, 21 Aug 2001 18:55:08 +0100*

If companies are using rot13 to "encrypt" copyrighted  
information, doesn't  
that make every unix user in the USA a criminal under the DMCA?  
It would be  
interesting to see what would happen to "the system" if a few  
million people  
went to the police and confessed...

---

## ⚡ Hack the Vote? Not in Broward County!

<james.paul@mail.house.gov>  
*Fri, 17 Aug 2001 23:03:31 -0500 (CDT)*

In [RISKS-21.61](#), Adam Shostack noted that Broward County was  
apparently going  
to let students have a crack at their new touch-screen voting  
systems. Bob  
Cantrell, director of intergovernmental affairs for the Broward  
Supervisor  
of Elections, claims that this will not happen. [Source:

William Welsh, 17

Aug 2001 \*Washington Technology\*, PGN-ed from

[http://www.washingtontechnology.com/news/1\\_1/daily\\_news/17017-1.html](http://www.washingtontechnology.com/news/1_1/daily_news/17017-1.html)]

---

## ✶ Re: Runway incursions

"Bill Hopkins" <whopkins@wmi.com>

*Fri, 17 Aug 2001 19:35:42 -0400*

The runway-incursion system that's behind schedule ([RISKS-21.60](#)) is the Airport Movement Area Safety System (AMASS). It uses data from the Airport Surface Detection Equipment (ASDE-3), a primary radar. "Primary" means it relies on reflections, not transponders, for detection and ranging.

It seems to me that any system that relies only on position tracking is going to have a tough time reliably detecting incursions without racking up lots of false alarms. The distance from the hold-short line to disaster is so small and the time to react so limited that the alarms have to be set to go off on very small changes. Variations in RF propagation, changing reflections from other moving aircraft (or service trucks), and system instabilities almost guarantee that they will when nothing is wrong. The technical folks may be able to tune each system to a level that ATC finds acceptable, but it will be slow, labor-intensive, frequent, site-specific, and expensive. Results will vary from facility to facility.

Much better systems are technologically feasible. Flight Management Systems know when the aircraft is stopped, when its brakes are off, when the engines are spooling up. A prototype FAA system controls red Runway Status Lights (RWSL) for visual back-up to "hold short" instructions, based on whom the controller has cleared to use the runway. The next generation aircraft radios have provision for addressable data link. Moving map displays are increasing common. Limited vocabulary speech understanding is increasingly reliable.

Mix these together with some intelligent design for the controller's display, and the runway monitor can raise a fuss when the pilot fails to acknowledge a "hold short", or the brakes come off too early, not when the radar jitters. Most operational errors by ATC and pilots will be prevented by putting redundant information where it is useful instead of relying on memory; others will be caught and corrected early. Life will be good. Stocks will rise. Politics will be civil. PGN's puns will all be funny. To all of us.

The risk: believing it might actually happen in our lifetime?

Bill Hopkins (whopkins@wmi.com, no longer in the ATC biz)

---

## **✶ Code Red 9? Code Crimson**

Alistair McDonald <alistair@bacchusconsultancy.com>

*Fri, 24 Aug 2001 16:06:13 +0100*

Two weeks into the Code Red exploit, when variant II or III or whatever you want to call it was particularly active, incidents.org noticed that another MS security flaw was being exploited. Their report is here <http://www.incidents.org/diary/august2001.php#132>. They give no data as to how many compromised systems are out there, possibly the reported probes are all an attempt to "jump start" the worm.

The vulnerability is described at <http://www.microsoft.com/technet/security/bulletin/ms01-023.asp>. Again, there has been a patch available for some time (since May, apparently), yet I'm sure that some systems will be unpatched. My Win2K SP2 machines did not need the patch, so I guess it's installed with SP2.

When will the world wake up and stop buying software from a software company that obviously can't write software well?

[Actually, the buying decision is probably done by people who know little about software, IMO].

Alistair McDonald, Bacchus Consultancy Ltd <http://www.bacchusconsultancy.com>

---

**⚡ AT&T - the computer MUST be right!**

"Sharon Mech" <sharon@cmhcsys.com>  
*Fri, 17 Aug 2001 17:26:03 -0400 (EDT)*

Our long distance service is plain, vanilla AT&T service. Long-distance charges appear on our local Ameritech phone bill. This past month, we got a bill showing charges for the AT&T One Rate plan, for which we had not signed up. (We also have an anti-slamming policy signed & on file.) So I called Ameritech. After negotiating their automated attendant hell, I was told that there was nothing they could do - I needed to call AT&T. At AT&T, more automated attendant hell. When I get the rep on the line, I give her my phone number and name, and explain the problem. She tells me that she can't help me, because our phone number has someone else's name on it, and neither I nor my husband is that person (whose name she will not reveal - I guess privacy does matter!) and she can't give me to a supervisor, thank you for calling AT&T! Just a note: We've lived at our house for 7 years, and always had the same area code and phone number. Apparently the AT&T record had been changed in February of this year, and our phone number was now associated with a different name and address. If there was a notation of who authorized the change, she sure didn't tell me - after all, it wasn't my phone line....

Back to Ameritech. Their rep confirmed that our line was indeed our line, in my name, at our address. I was fortunate - this rep had initiative. Once I explained the situation (took a couple of repeats) he put me on hold & called AT&T to set up a conference call. Things almost fell apart at this point, because Ameritech reps have a pretty strict time limit on

their  
calls. We got an AT&T rep on the phone at just about the limit.  
He went on  
to explain to the AT&T rep that my line was really my line. She  
wasn't  
buying it - after all, her computer MUST be right, but finally  
grudgingly  
agreed to amend her record, noting his ID, info, etc. as  
justification. Finally we could get to the point of removing the  
unwanted  
calling plan. Mission accomplished. One last detail - the  
calling plan cost  
a certain amount, but also involved a credit. Because the plan  
changes  
tariffs & long distance rates, our long- distance usage  
(minimal) had been  
billed at the wrong rate, and neither of the reps could tell me  
what we  
actually owed.

Sharon Mech <sharon@cmhc.com>

---

## ✦ **Re: DejaGoogle rides again (Weingart, [RISKS-21.61](#))**

"Leeming, Geoffrey" <gleeming@lehman.com>

*Mon, 20 Aug 2001 08:59:45 +0100*

What risks? If you read a post in Deja/Google it gives you a  
nice link to  
the rest of the thread. Full marks to Google for only giving  
one link to  
the thread as a whole, not one to each of the entries. If it  
had been the  
wrong thread, getting one link to each entry would have meant  
that the next  
search result would have been pushed way down the list.

Geoffrey Leeming, Technical Security Manager

Lehman Brothers International Ltd. +44 (0) 20 7260 1338

[Also noted by several others. PGN]

---

## ⚡ Re: Risks of automated junk/spam filters (Loftis, [RISKS-21.60](#))

AlphaLau <avlxyz@yahoo.com>

Wed, 22 Aug 2001 09:14:01 +0100 (BST)

Unfortunately, this happens with Yahoo Mail as well. Their "Bulk Mail" feature is similar, and you used to be able to specify if an email was indeed not spam. Of course what they actually did with it...

Y!Mail also has a nifty "Block email from this Address" feature that will send email with those addresses into a blackhole.

I have suggested to Yahoo to keep a log of blackholed emails, just the date, from, to & subject fields should be enough. All I got in reply was, that is how the blocking works. Use Y!Mail Filter to manually handle it.

So in effect, users are saddled with 2 spam "features" that are not really useful. I have disabled both.

Still, Y!Mail is one-up on Hotmail with it's block-mail feature! :)

Alpha

---

## ⚡ Yet another MS Hotmail risk

Kimmo <kimmo.pyykko@sonera.com>

Mon, 20 Aug 2001 17:44:25 +0300

One addition on Michael Loftis' article about MS's Hotmail service

(<http://catless.ncl.ac.uk/Risks/21.60.html#subj11>):

I also have a Hotmail account to handle the private mail and I noticed today an interesting behaviour concerning the Junk Mail-folder:

Now, logging in this morning (Aug 20) I noticed a warning mail from Hotmail Staff (Aug 18) that my account size is too large. Opening the mail was impossible, because all I got was a warning that I was 5120K over my quota. Someone's spam bot had gone to overdrive and sent over 600 spams to my account (all similar and from the same address, size about 10K).

Emptying the Junk Mail folder (and blocking the spammers address) meant that I could again use my account normally and also read the mail from Hotmail Staff, which told me that if I didn't react before Aug 23, Hotmail would start "deleting messages (usually older ones from all of your folders) until your account is smaller than the 2-MB size limit".

Apparently, this is normal behaviour for MS Hotmail, as I managed to find out in the service conditions. 5 days reaction time, before we start emptying your account starting from the oldest. The risk?

If someone does not check his/her Hotmail for a week (eg.

vacation,  
illness), it is very easy to remove all his/her mail from all the  
folders by simply sending in too much spam. Including the Junk  
Mail-folder into the account size limit makes this kind of  
"denial-of-mail" very easy, because mail in a Junk Mail folder  
isn't  
deleted for 14 days from it's arrival.

Fortunately, I don't trust WWW-based email services enough to  
use them  
for anything important but still: wiping out your email box is a  
nuisance.

Kimmo Pyykkö, Development Manager, New Communications Services/  
Technology Center tel. +358 2040 58328

---

## **✶ REVIEW: "SSL and TLS", Eric Rescorla**

Rob Slade <rslade@sprint.ca>  
*Mon, 20 Aug 2001 10:42:59 -0800*

BKSSLTLS.RVW 20010607

"SSL and TLS", Eric Rescorla, 2001, 0-201-61598-3, U\$39.95/C  
\$59.95

%A Eric Rescorla ekr@rtfm.com

%C P.O. Box 520, 26 Prince Andrew Place, Don Mills, Ontario  
M3C 2T8

%D 2001

%G 0-201-61598-3

%I Addison-Wesley Publishing Co.

%O U\$39.95/C\$59.95 416-447-5101 fax: 416-443-0948

%P 499 p.

%T "SSL and TLS: Designing and Building Secure Systems"

The preface states, quite clearly, that this is a work for  
designers,  
programmers, and implementors. In other words, it's a very  
technical

book. Even the preface, though, is written with a clarity that is unusual, and refreshing, in technical literature.

Chapter one provides some background to communications security and encryption. The material is demanding, and is definitely not a primer. A number of items are glossed over, but the persistent reader should be able to glean some very solid explanations of important concepts. The "family tree" of SSL (Secure Sockets Layer) is given in chapter two, with a description of the development steps along the way. Chapter three outlines the basic, or most common, mode of SSL, and then provides details about specific aspects of the algorithms and data structures used at different points. Various options and extensions, for a number of functions, are described in chapter four. The security of the SSL system itself, as opposed to the security it provides for transactions, is thoroughly examined in chapter five. Chapter six is an examination of performance issues, and the ways in which execution can, and can't, be improved.

SSL is, of course, only a protocol and not a full application. Design considerations for effective use within a system are detailed in chapter seven, and sample C and Java code for effecting the operations is given in eight. SSL was designed for, and is most widely used with, HTTP (HyperText Transfer Protocol), and chapter nine details the requirements and difficulties of using the system to secure Web communications. Chapter ten uses SMTP (Simple Mail Transfer Protocol) as an example of the use of SSL to protect other communications operations. Finally, Rescorla compares SSL to the major competing

systems of IPsec, S-HTTP (Secure HTTP), and S/MIME. (It is nice to see that the author identifies his own potential bias in the debate.)

This book is aimed at a technical audience, and members of that group will undoubtedly welcome it. However, the lucid presentation, and range of security concepts covered make this a useful reference for many others. Those involved in online commerce and the necessity to secure transactions over insecure links will find solid discussions addressing those issues. Security analysts and practitioners may be challenged to look into the internals of systems generally examined only at a superficial level. And anyone interested in the security of the Internet will find a clear and fascinating review of its underpinnings.

copyright Robert M. Slade, 2001 BKSSLTLS.RVW 20010607  
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>

---

## **✶ Dependable Systems and Networks DSN-2002 Call for Contributions**

Anup Ghosh <aghosh@cigital.com>  
*Thu, 23 Aug 2001 08:31:18 -0400*

The International Conference on Dependable Systems and Networks  
(DSN-2002)

Bethesda, Maryland, USA      23-26 Jun 2002      <http://www.dsn.org>  
Full papers and workshop proposals due 19 Nov 2001

This conference has combined the International Symposium on Fault-Tolerant Computing (FTCS), the Working Conference on Dependable Computing for Critical Applications (DCCA), into the DSN track now called Dependable Computing and Communications, and in 2002 will also include the International Performance and Dependability Symposium (IPDS). See [www.dsn.org](http://www.dsn.org) for submission information. [PGN-ed for RISKS]



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 21: Issue 63**

**Saturday 1 September 2001**

## Contents

- [The Heavens at War: NMD assessed](#)  
[Pete Mellor](#)
- [SDI chief says system may not be reliable](#)  
[PGN](#)
- [Federal tax returns missing in Pennsylvania](#)  
[PGN](#)
- [Hotmail hackable with one line of code](#)  
[NewsScan](#)
- [Even dead people use Microsoft software](#)  
[Jeremy Epstein](#)
- [More interesting MS certificates](#)  
[Stuart Prescott](#)
- [Directory service based on car license plate](#)  
[Ulf Lindqvist](#)
- [Re: Air Force office mails confidential information ...](#)  
[Jay D. Dyson](#)
- [Info on RISKS \(comp.risks\)](#)

---

**✶ The Heavens at War: NMD assessed**

Pete Mellor <pm@csr.city.ac.uk>

Wed, 29 Aug 2001 11:44:20 +0100 (BST)

The Heavens at War: BBC Radio 4, 28th August 2001  
Reporter and presenter: Jackie Hardgrave.

## Preface

The following summary is based upon notes made while listening to the first broadcast of the programme, together with reference to the web-site (which does not include a full transcript). It is as fair a summary of the content of the programme as I could manage. However, shorthand is not one of my many talents, and I cannot claim total accuracy. I stand to be corrected if I have misquoted or wrongly attributed a quotation. I have indicated uncertain spellings of people's names by (sp?).

I have placed my own comments in brackets: [PM: my comments] and added some more at the end.

Please see the web site:

[http://www.bbc.co.uk/radio4/atoz/heavens\\_at\\_war.shtml](http://www.bbc.co.uk/radio4/atoz/heavens_at_war.shtml),

or listen to the repeat broadcast on Sunday 2nd September at 5pm (British Summer Time).

## Introduction

The programme concerned the National Missile Defense system (NMD). [PM: It used that name throughout, although the "National" has now been dropped and it is known as "Missile Defense System" (MDS), I believe.] This is also

known as "Son of Star Wars" after the nickname for the President Reagan's earlier Strategic Defense Initiative (SDI).

Main question: Will the technology work or is it doomed to expensive failure?

The threat to the US is now perceived to be from "rogue states" and no longer an all-out nuclear strike from Russia. North Korea, Iran and Iraq were specifically mentioned. Also, although China and Russia have sophisticated systems, an accidental launch is a possible threat.

In 1972 only 9 nation states had the capability to launch an intercontinental ballistic missile. This number has vastly increased.

Around 1000 ICBMs were produced last year. Their range is continually increasing (e.g., N. Korea has tested a missile with an intercontinental (IC) third stage). There is also the possibility that the possession of intercontinental missiles may be used in diplomatic blackmail to deter the USA from some course of action.

Michael O'Hanlon, a Senior Fellow in Foreign Policy Studies at The Brookings Institution (a private institution that studies public policy), gave the example of Iraq launching a new but limited attack on the Kuwaiti oilfields in 10 to 20 years time. If Iraq was by then capable of launching missiles at the USA, and a new "Desert Storm" was on the way, Saddam Hussein (or Uday, who might have taken over by then) would see no reason not to "play for keeps" and threaten to launch an ICBM attack, or actually attack a small

city as a demonstration of what they could do.

President Reagan began the original "Star Wars" -- which failed due to financial [PM: and technical?] reasons. Why is "Son of Star Wars" under way now? 1998 was a pivotal year. India and Pakistan both tested nuclear warheads. The Rumsfeld (sp?) commission reported that a nation could easily develop the capability to produce nuclear warheads and then surprise the West by suddenly testing them. China was suspected of having obtained the nuclear secrets of the USA by espionage.

### The Technical Dimension

There are three phases in which to destroy an ICBM launched against one's territory:-

1. On first launch, before the missile has left the atmosphere. This provides a very short window of opportunity, but the missile is relatively easily detectable by the plume of exhaust gases from the boosters or first stage launch vehicle.
2. In mid-course, after the missile has left the atmosphere and is following a ballistic trajectory through space. This offers the easiest opportunity, since it is the longest phase. During this phase the missile might break up, and release its warheads and "decoys" (see below) to follow their separate paths.
3. After reentry into the atmosphere when the missile is minutes away

from its target. By this stage, the missile will almost certainly have broken up (if it is going to do so), releasing its lethal payload along with its decoys.

Three interception test have been conducted so far. [PM: I believe these were mid-course.] Two failed, and the third (a few weeks ago) succeeded [PM: but this "success" has been questioned!].

NMD requires long-range interceptor missiles to destroy hostile ICBMs. The interceptor releases a "kill vehicle" which homes in on, and collides with, the incoming ICBM. No explosives are involved. The concept has been described as a "smart rock" or a "bullet to hit a bullet". [PM: the term "smart rock" cropped up in the earlier SDI also.] A total of 250 interceptor missiles with kill vehicles are to be deployed in Alaska and Florida (?).

Incoming ICBMs will be detected by ground-based radar and by satellite-based infrared sensors. Nine new radar systems will sort warheads from decoys. Satellite-based infrared sensors will assist interception in outer space. The problem here is that heavy objects (e.g., nuclear warheads) have the same trajectory as light objects. The incoming ICBM could therefore deploy light weight decoys in large numbers without sacrificing range. For example, decoys could be mylar balloons with aluminium coating. Dozens of these could be released.

In some cases, it may be necessary to launch several interceptors.

Philip E. Coyle, an advisor to the Center for Defense Information (an independent Military Research Organisation) and until recently the director of Operational Test and Evaluation at the Pentagon, with responsibility for overseeing NMD testing, gave the "hole in one" analogy. Hitting an incoming ICBM is like trying to score hole in one (you only get one shot!) on a golf course where the hole is moving at 15000 mph. With decoys, this is like having a lot of holes with flags to aim at and having to choose the right one at the same time! The problem would be very different in a real situation (unlike the tests conducted so far). Not all eventualities can be planned for.

Lisbeth Gronlund, Senior Staff Scientist of the Union of Concerned Scientists, pointed out that any nation that was capable of missile production would find the production of balloon decoys a trivial problem.

The tests so far have used decoys, and in the successful test the kill vehicle did pick the correct target, but this was not a realistic test, since the "warhead" was different in appearance and temperature to the decoys [PM: presumably to a degree greater than that which the designers of a real attacking ICBM could achieve?].

At least one of Coyle and Gronlund suggested that NMD will never be tested in realistic conditions before being deployed, since it would almost certainly fail!.

O'Hanlon's views partly agreed with this. NMD cannot be tested in a totally real situation. However he believes that it is possible to get close to it, for example by not telling the "defenders" when the "hostile" missile that is their target is to be launched and what decoys it will deploy. He stated that, although it would be a delusion to assume that 100% success could be guaranteed, a 95% confidence in a NMD system would be better than no defence at all. [PM: See below!]

The Ballistic Missile Defense Organization adopts a more bullish position: a solution to all of these problems will be found. One telling quotation (unattributed) was: "The United States will do what the United States has to do!" Anyway, the adversary will take time to prepare and test counter-measures, and this activity will betray itself to the intelligence agencies.

However, there is a more serious problem if the ICBM carries a lethal chemical or biological payload. Unlike a nuclear warhead, which is an integrated complex device, the lethal material is just "stuff". The payload could divide up into twenty or more bomblets which would be released and would fan out over the target area. These would all be identical in appearance, all real, and all lethal.

Faced with this possibility, the defenders' best tactic is to strike immediately after launch, while there is only one target. This requires an interceptor missile close to the point of launch. In practice,

this means  
on board a ship. President Bush has approved the budget to  
develop this  
capability. However, neither the ships nor the missiles they  
will carry  
have yet been developed, and they will not be ready for service  
for many  
years.

Tom Colleenor (sp?) pointed out that a strike in the first stage  
after  
launch would allow only a minute or two to decide whether to  
launch the  
interceptor, which means that the decision must be taken by a  
field  
commander. [PM: This has interesting political and strategic  
military  
implications!]

For a more "Star Wars" approach the team visited Kirkland Air  
Force base in  
New Mexico to observe developments in a real "ray gun": the use  
of a laser  
beam strike against an ICBM. Undergoing development is the  
Airborne Laser  
(ABL) on B747 aircraft. This consists of four lasers, three to  
track the  
missile and one to kill it with a one million watt bolt of  
energy. The  
attack would proceed as follows: the launch of the hostile ICBM  
is detected  
by infrared sensor detection (IRSD) [PM: on the aircraft or on  
satellite?].  
The aircraft uses its tracking lasers to get the range and  
bearing and locks  
on to the exhaust plume. It then aims its large laser in the  
nose of the  
aircraft at the plume and tracks up to the nose of the missile  
and unleashes  
its energy. The effect is not to destroy the missile in a  
sudden explosion,  
but to heat the fuel tanks to the extent that they develop  
cracks and so to

cause a structural failure.

It will take many years for this to become ready for combat. In the meantime, spin-offs in smaller tactical or space-borne lasers might provide some returns. [PM: Space-borne lasers were a feature of the original SDI. These were to be mounted on orbiting robotic "battle stations". One proposal (which was the subject of actual nuclear tests) was that the gamma radiation from a nuclear explosion could be harnessed into a single collimated beam which would fry everything in its path. A battle station carrying such a weapon would obviously be a "one-shot" device!]

Joe Cirincioni (sp?) pointed out that, also in the meantime, the bad guys could develop a few simple counter-measures such as polishing the nose-cone to reduce absorption of radiation, spinning the missile (not as easy as it sounds) to avoid overheating of any one part of the surface, or insulating it with a coating (such as cork!) to avoid things getting too hot.

President Bush is apparently willing to spend, spend, spend his way around these minor technical problems.

### The Political Dimension

OK. So what is there for us to worry about here? Answer: Lots! [PM: "Us" seemed to mean Europeans. However, most of the worried voices on the programme were American, which could be good news.]

NMD will breach the 1972 Anti-Ballistic Missile (ABM) treaty by

end of this year if the Bush administration pursues its present course. The pro-ABM argument is that the treaty achieved a stable stalemate between the two nuclear superpowers during the cold war by preventing either from developing an effective protection system from behind which to launch a pre-emptive nuclear strike, and that it still operates to forestall an offensive arms race.

The opposing view was put by Senator Kyle, who argued that the ABM treaty was useful only in the cold war when there were only two nuclear superpowers and that it is no longer relevant. He went on to argue that the treaty was not a cause of stability, and that the offensive arms race continued with the treaty in place. In fact, it locked the superpowers into a strategy based on mutually assured destruction (appropriate acronym: MAD): If you wipe us out, we'll wipe you out, and then we'll all be dead! This no longer makes sense, since there is no longer a monolithic enemy on the other side of an Iron Curtain. The rules have changed, and we in the US will act in our interests, not Russia's nor anyone else's. Russia cannot veto NMD, and indeed, the only sanction it could threaten is a renewal of an offensive arms race which it can no longer afford.

President Putin is less than chuffed about this! There is some hope that a detente might be reached around a trade-off of NMD and nuclear weapons reduction, but the USA is currently gung-ho for its impenetrable shield.

O'Hanlon was worried that NMD might jeopardise attempts to work with Russia to control, stabilise, and (eventually) decommission (or at least reduce) its nuclear arsenal. It still holds thousands of nuclear warheads mounted on ICBMs. These constitute a hair-trigger weapon which could be aimed at the West in an instant. [PM: Russia announced several years ago that its nuclear missiles were no longer aimed at the West. Unfortunately, to re-aim them would take about as long as it takes to download the software. How long did your last reboot take? Another small point is that many of the weapons are in the territory of (and under the control of?) newly independent and politically unstable states which are ex-USSR.]

O'Hanlon said that the fact that the ABM treaty is 30 years old does not make it a "relic". His mortgage is 30 years old, but is still not a relic, and the Constitution of the United States is even older, but is still regarded as a useful document.

He cited an interesting example. In 1998 a "sounding" rocket launched from Norway was mistaken for a US attack vehicle by the Russian defences. They were minutes from a retaliatory launch when the mistake was discovered.

Ivan Zifrancuk (sp?), a Russian defence expert, was interviewed to give the Russian point of view.

America's allies are also worried. Radar bases and communications in the UK are needed for tracking. The Menwith Hills installation has been the target

of a Greenpeace protest. [PM: The compliance of the present British government is remarkable, given the likelihood that the presence of tracking stations will make Yorkshire a primary target for America's enemies. France and Germany have been more outspoken.]

Phyllis Starkey MP was interviewed and stated that in her opinion NMD was a destabilising influence, and that the British Government should look to British interests

O'Hanlon cited the problem of China (particularly sensitive since the loss of one of its fighter aircraft in collision with a US spy plane earlier this year). The Bush administration has taken pains to reassure the Chinese (as it has the Russians) that NMD is not an offensive capability aimed at them.

Unfortunately, there is a long-standing dispute over Taiwan, and in the medium term NMD could be capable of neutralising the effect of Chinese missiles. At the last count, China had only 20 missiles capable of reaching American soil. Senator Kyle stated that the USA would never tolerate a military take-over of Taiwan by China, and would come to its defence. The existence of NMD would therefore be perceived as a threat by China, and may provoke an arms race with China.

## Conclusion

The old competition between predator and prey, between defence and offence, between the baron in the castle and the besiegers using

the siege catapult were quoted. The difference here is that the "castle" in this new cycle of competition cannot be built without the expenditure of billions of dollars, whereas the "catapult" (the means of penetrating or circumventing NMD) are relatively cheap. So where is the money to come from? Step forward the loyal, long-suffering (and notoriously tight-fisted) US taxpayers! President Bush has promised to lighten their burden. Is NMD consistent with this?

As the programme concluded: "The world awaits your decision!"

= = = = = Peter Mellor: Personal Comments = = = = =

The Missing Dimension: Safety, Reliability, and Software

When President Reagan launched the Strategic Defense Initiative (SDI, aka "Star Wars"), it was intended to provide an absolutely impregnable defence for the USA against ICBM attack.

It was widely regarded as utterly fantastical in conception, absurdly expensive to design and construct, impossible to test, and ineffective for its intended purpose.

An impregnable defence must have a negligible probability of letting one attacking missile through. O'Hanlon states that a "95%" confidence is better than no defence at all. Where thermonuclear devices are concerned, a 1% failure rate under mass attack means that you might as well not have bothered. (I saw a bumper-sticker in California which read: "A single

nuclear device can really spoil your day". I agree!) To destroy the USA, only four devices are required, one at each corner, in the stratosphere, outside US territory. The electromagnetic pulse would cause an electrical potential spike which would zap every non-hardened semiconductor device in the country. Eight out of every ten dollars would disappear in an instant. (Think about it!) Hitler gave up on the air assault on Britain since he realised he could not cope with a 10% attrition rate on the raiding forces. Now we need a 99.9999% (or higher) attrition rate.

The NMD is a cut-down version of SDI. At least we no longer have to contend with the spectre of a world patrolled by ever-alert robot battle stations in orbit armed with thermonuclear devices to deliver collimated gigawatt doses of energy to anything which ascends above 50,000 feet and rail-guns firing several thousands of rounds per second of hypersonic projectiles at any suspect object in orbit.

The NMD proposals are less fantastic, but perhaps the more dangerous for being slightly more plausible.

What SDI and NMD have in common is that they are both crucially dependent on software for command and control.

The head of software development for SDI was David L. Parnas. Once he became aware that the current software development methods could not yield the impossibly high reliability required for SDI, he did the decent thing and resigned. He did so very publicly and published his reasons

for  
becoming totally disillusioned with the farcical SDI enterprise  
in a  
brilliant essay in which he stacked up each one of the then  
popular methods  
and showed why it was doomed to fail. [As I recall, David was  
merely on a  
review panel, not head of development. PGN]

His resignation and essay probably did as much to scupper SDI as  
its  
ludicrous and exponentially increasing cost.

Now, either we have solved all of the problems with developing  
high-integrity real-time embedded software in the few years  
since SDI was  
abandoned (and I don't believe it for a nanosecond), or we are  
into another  
technically infeasible and ultimately farcical project.

I have seen no discussion of NMD in the safety-critical systems  
list  
recently, and no criticism anywhere from the reliability and  
safety  
viewpoint. (It was not even mentioned in the BBC Radio 4  
programme "The  
Heavens at War" that I have summarised above.)

The silence is deafening!

Peter Mellor, Centre for Software Reliability, City University,  
Northampton Square, London EC1V 0HB  
Tel.: +44 (0)20 7040 8422 ) NOTE: Code recently changed from  
Fax.: +44 (0)20 7040 8585 ) 7477 to 7040  
e-mail: Pete Mellor <p.mellor@csr.city.ac.uk>

---

## **✶ SDI chief says system may not be reliable**

"Peter G. Neumann" <neumann@csl.sri.com>  
*Wed, 15 Aug 2001 18:31:22 PDT*

The head of the Pentagon's missile defense programs said he is not fully confident in the "basic functionality" of the anti-missile system that successfully intercepted a mock warhead in space last month. That is why the next test of the system, scheduled for October, will be a replay of the July 14 test, with no additional complexities such as putting more decoys aboard the target missile, Air Force Lt. Gen. Ronald Kadish, director of the Ballistic Missile Defense Organization, told a group of reporters. "It is still not totally comfortable for me to say that we can make the hit-to-kill technology work consistently, even in that simple scenario," Kadish said, adding later, "We still need some more reliability in there." [Source: AP item, Missile Defense Chief 'Not Totally Comfortable' With Reliability of Anti-Missile System, 15 Aug 2001; and then, there are reports of the GPS-aided homing beacon that aided the tests -- even the two that failed! PGN]

---

## **✶ Federal tax returns missing in Pennsylvania**

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

*Wed, 29 Aug 2001 20:00:05 -0700 (PDT)*

As many as 40,000 federal tax returns [earlier thought to be only 1800] and tax payment checks totaling more than \$800 million from New England and

upstate New York have been lost or destroyed at a processing center operated by the Mellon Bank in Pittsburgh for the Internal Revenue Service. One source was quoted as saying, "The system was flawed. It gave them incentive to stick the payments in a drawer. It was almost cost-effective for Mellon to do that. There was no reward for timely processing." (A somewhat similar case at the IRS Philadelphia center in the mid-1980s was also noted.)  
[Source: Albert B. Crenshaw, \*The Washington Post\*, 30 Aug 2001; Page E01]

---

## **🔥 Hotmail hackable with one line of code**

"NewsScan" <newsscan@newsscan.com>  
*Fri, 31 Aug 2001 10:35:17 -0700*

Security consultant Jeremiah Grossman was able to break through Microsoft's Hotmail and Passport protection schemes with just one line of code. Microsoft has patched the code, but Grossman says he could do it again in 8 hours of work. His hacking experiment used a "cross-site scripting" technique that attaches invasive code onto programs used to make Web pages more interactive. Grossman calls them "a breeding ground for new types of Web security vulnerabilities," and Shawn Hernan of the Computer Emergency Response Team at Carnegie Mellon University says that "it's easy to dream up very, very bad scenarios."  
[\*USA Today\*, 31 Aug 2001; NewsScan Daily, 31 August 2001]

<http://www.usatoday.com/life/cyber/tech/2001-08-31-hotmail-security.htm>]

---

## ✶ Even dead people use Microsoft software

"Jeremy Epstein" <jepstein@webmethods.com>

*Fri, 24 Aug 2001 10:19:27 -0400*

Computerworld reports that a Microsoft letter-writing campaign opposing the anti-trust actions used the names of dead people. The Utah Attorney General, who received the letters, was not amused. Other Attorneys General received duplicate letters with similar problems. MSFT says they didn't do it, but pointed to "Citizens Against Government Waste" which is a leading the effort.

([http://www.computerworld.com/storyba/0,4125,NAV47\\_STO63256,00.html](http://www.computerworld.com/storyba/0,4125,NAV47_STO63256,00.html))

The risk is that any sufficiently automated letter writing system is going to eventually screw up and get caught. Dead people don't handwrite letters.

---

## ✶ More interesting MS certificates

Stuart Prescott <s.prescott@ysa.org.au>

*Fri, 24 Aug 2001 10:32:53 +1000*

I noticed today that the Microsoft WindowsUpdate site was

offering a Service Pack 2 for Internet Explorer, and since a number of our machines here use IE5.5 I decided to have a look at what "functionality" it offered. As with all downloads from WindowsUpdate, they are cryptographically signed; however, this time some of the components were signed by "IE Beta Division", with a certificate authority of "IE Beta Division"... i.e. (PGN: pardon the pun) the certificates are not trustworthy.

The RISKS? Naturally, there are issues here in verifying that these updates are actually from Microsoft. Then there are the RISKS of users saying "No" to installing the badly signed bits and possibly ending up with a (more) broken IE installation. Or there is the RISK of users becoming used to dismissing error messages....

I didn't realise that MS and IE could become even scarier with time...

---

## **✶ Directory service based on car license plate**

Ulf Lindqvist <ulf@sdl.sri.com>  
*Mon, 27 Aug 2001 09:38:03 -0700 (PDT)*

>From Swedish newspaper \*Aftonbladet\* Aug 27, 2001,  
<http://www.aftonbladet.se/vss/nyheter/story/0,2789,84644,00.html>

In Sweden, a new type of directory service will soon be introduced by the company Ahhaaa [yes, that actually seems to be their name, see <http://www.ahhaaa.com/> ]. You will be able to call this service

24-7, give the license plate number of a car, and they will immediately tell you the name, address and phone number of the person registered as owner of that car. If the owner is a business, they will also tell you the number of employees and annual revenue.

The article states a number a "benefits", such as calling the driver who just cut you off to complain, locate parking violators or notify an owner whose car has been broken into. Last but not least, the article suggests that if you find another driver attractive, this service would make it easier to make contact.

It does not take a criminal mastermind to see ample opportunities for abuse - road rage, stalking, fraud etc. One could argue that this information has always been available to the public in Sweden, albeit from different sources (see <http://justitie.regeringen.se/pressinfo/pdf/publicaccess.pdf> for an explanation of the Swedish Principle of Public Access to Information). However, with modern technology, deregulation of telecommunication services, and the ubiquitousness of mobile phones, the information is instantly available and therefore the opportunities to act on impulse are much greater.

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: Air Force office mails confidential information ...

"Jay D. Dyson" <jdyson@treachery.net>  
Sat, 25 Aug 2001 19:30:05 -0700 (PDT)

Jim Griffith ([RISKS-21.62](#)) noted an Air Force Academy officer accidentally sent confidential information about some 40 cadets to all 4400 cadets at the school.

This incident sounds suspiciously like a Sircam worm infection of the officer's system. First off, I doubt that e-mail is typically utilized to send out such reports since such confidential information should never be sent in the clear. Secondly, how else can the Air Force explain the means by which the mail was so readily disseminated?

I don't believe we're being told the whole story here. And I believe an officer is being let off the hook when he should be nailed for actions that are tantamount to criminal negligence.



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 21: Issue 64**

**Saturday 1 September 2001**

## Contents

- [Temelin nuclear plant software problem](#)  
[Pete Mellor](#)
- [Blame the victim: vandalized Web sites may be liable for damages](#)  
[NewsScan](#)
- [More risks when driving](#)  
[Martin Cohen](#)
- [Risks of "pre-owned" computers](#)  
[Nick Brown](#)
- [Microsoft Reader e-books broken](#)  
[David Farber](#)
- [AOL silently dropping mail](#)  
[Simon Waters](#)
- [eBay fails to protect email addresses of users](#)  
[Vassilis Prevelakis](#)
- [Re: Avoiding prosecution of the DMCA](#)  
[A J Stiles](#)
- [Risks and madness on the BT Cellnet site](#)  
[Mike Perry](#)
- [Not such an equal opportunity](#)  
[Bill Lamb](#)

- [Re: Code Red 9? Code Crimson](#)  
[Bob Frankston](#)
  - [Risks of outsourced check verification](#)  
[Peter Simpson](#)
  - [Can't hold room, but can bill](#)  
[Sandy Antunes](#)
  - [Caller ID vs. ANI confusion, again](#)  
[William Kucharski](#)
  - [Re: Mixing advertising and credit-card activation](#)  
[John Clarke](#)
  - [REVIEW: "Information Security Management Handbook", Tipton/Krause](#)  
[Rob Slade](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

## ⚡ **Temelin nuclear plant software problem**

Pete Mellor <pm@csr.city.ac.uk>  
*Mon, 27 Aug 2001 15:04:35 +0100 (BST)*

The following is one item from the regular news digest produced by the students of Charles University, Prague:-

CAROLINA No 429, 24 Aug 2001  
FROM THE EVENTS OF THE PAST TWO WEEKS (August 9 - August 22)

Temelin up Again, down Again

The Temelin nuclear power plant was activated again 12 Aug 2001 after three months of repairs to a vibrating turbine (see Carolina 428). The relaunch of Temelin provoked hostile reactions from some Austrian politicians and anti-nuclear and environment activists.

News leaked 15 Aug about new vibrations in the turbine, which caused an

18-hour shutdown. However, plant officials claimed the shutdown was used to "balance a rotary part in the turbine." The reactor 19 Aug was automatically switched off due to a software error in a steam-delivery regulator.

Temelin opponents claimed this shutdown was the 23rd since the beginning of operating tests. According to Temelin management, the shutdowns are a normal part of the testing procedure and are not related to nuclear safety problems. Temelin CEO Frantisek Hezoucky said Temelin is exceptional only in one respect: it is the very first nuclear power plant where its testing is broadcast live to the public.

STUDENTS' E-MAIL NEWS FROM THE CZECH REPUBLIC

Charles University in Prague, Faculty of Social Sciences

Smetanovo nabr. 6, 110 01 Prague 1, Czech Republic

e-mail: CAROLINA@mbox.fsv.cuni.cz ISSN 121-5040

tel: (+4202) 22112252, fax: (+4202) 22112219

---

## **✶ Blame the victim: vandalized Web sites may be liable for damages**

"NewsScan" <newsscan@newsscan.com>

*Mon, 27 Aug 2001 11:00:13 -0700*

Some legal scholars are suggesting that a Web site vandalized by hacker attacks may itself be legally liable if its customers suffer damages and if the site was negligent in maintaining security. Law professor Margaret Jane Radin of Stanford University predicts: "A court is going to say

it is negligent of you not to implement preventative measures if they are reasonably effective and affordable." No reported court decisions have dealt with the issue, but Radin says that lawsuits in the near future are highly likely to be lodged against companies and network providers targeted by "denial of service" attacks. [*The New York Times*, 24 Aug 2001; NewsScan Daily, 27 August 2001 <http://partners.nytimes.com/2001/08/24/technology/24CYBERLAW.html>]

---

## **⚡ More risks when driving**

Martin Cohen <mjcohen@mediaone.net>  
*Sat, 18 Aug 2001 01:31:48 GMT*

*The New York Times* e-mail version contained an ad offering to teach you a language while you are driving. Imaging trying to learn an irregular verb while negotiating difficult traffic.

[You might drive right through a subjunction. Incidentally, someone was jogging toward me this morning when his cell phone rang. At least he had the good sense to stop running. PGN]

---

## **⚡ Risks of "pre-owned" computers**

BROWN Nick <Nick.BROWN@coe.int>

*Sat, 1 Sep 2001 13:55:20 +0200*

The BBC reports that "confidential files containing the identities of alleged paedophiles and their victims were found on a second-hand computer bought from Bristol University".

Full story at [http://news.bbc.co.uk/hi/english/uk/newsid\\_1519000/1519889.stm](http://news.bbc.co.uk/hi/english/uk/newsid_1519000/1519889.stm)

Not a new RISK, but the first time I've seen this particular combination.

Does *\*your\** local social welfare department, public hospital, or police station have a statutory duty (in the interest of the taxpayers) to sell, rather than destroy, old equipment ? And if so, is there a mandatory procedure for securely erasing the hard disk first ?

Nick Brown, Strasbourg, France.

---

## **Microsoft Reader e-books broken**

David Farber <dave@farber.net>

*Fri, 31 Aug 2001 23:51:19 -0400*

An anonymous programmer has found a way to decrypt Microsoft Reader e-books on Windows PCs, but has not released it.

[Source: Breaking Microsoft's e-Book Code, By Wade Roush, Technology Review,

30 Aug 2001, <http://www.technologyreview.com/web/roush/roush083001.asp>;

PGN-ed; Dave has been predicting this, but then all lame

protection seems

to be easily broken, relying on the DMCA for protection.

Dave's archives

are at <http://www.interesting-people.org/> . PGN]

---

## **✶ AOL silently dropping mail**

Simon Waters <Simon@wretched.demon.co.uk>

*Sat, 25 Aug 2001 23:49:09 +0100*

I received reports from an AOL user of e-mail's not getting through.

Checking log files show that AOL's mail server had received all the messages correctly.

Queries to AOL's postmaster account received no response.

Web pages run by AOL users suggest the cause of this is that I may have triggered a "suspicious relaying" trap with the AOL server.

Assuming this is the case it is interesting that AOL choose to drop the mail silently, when all the information required to make such a decision is available to the mail transport agent before the body of the mail is sent. Thus AOL could choose to refuse the mail politely, using less bandwidth, and informing the sender of a problem, but prefer to waste bandwidth and delete the e-mail silently.

The Risk? Assuming AOL cares enough about their subscribers e-mail not to delete it without notifying sender or recipient, or answer questions on the

topic. The only way I can see to mitigate the risk is to switch to another ISP.

+44(0)1395 232769

Moderated discussion of teleworking at news:uk.business.telework

---

## **✶ eBay fails to protect email addresses of users**

Vassilis Prevelakis <vassilip@dsl.cis.upenn.edu>

*Sun, 26 Aug 2001 18:01:09 -0400 (EDT)*

Normally eBay will not disclose the email addresses of its users. When you wish to send email to an eBay user, eBay provides a proxy service accepting the email and then forwarding it to the recipient.

However, if the mailhost for the recipient is down or unavailable, the sender will get a warning email saying that the original message could not be delivered but the system will go on trying, WITH THE E-MAIL ADDRESS OF THE RECIPIENT.

Another example of not thinking things through.

Vassilis Prevelakis, Distributed Systems Laboratory, Univ. of Pennsylvania  
Philadelphia, PA 19104-6389 +1 215 898 0375 vassilip@dsl.cis.upenn.edu

---

**✶ Re: Avoiding prosecution of the DMCA (Re: Petrou, [RISKS-21.62](#))**

"A J Stiles" <ajs2@adyx.co.uk>

Sun, 26 Aug 2001 11:59:03 +0100

But you are forgetting the law of Dual Criminality. A person can only be extradited from one country to another if what the person did was recognised as a criminal offence in the country where they did it. Since pointing out a security vulnerability is not a criminal offence in most countries, extradition can be refused. (Otherwise anyone who drinks alcohol could be extradited to any muslim country and executed!)

Of course, the USA could act illegally (as it has done on many occasions in the past). That would technically be an act of war .....

A J Stiles <ajs2@adyx.co.uk> <http://pages.zoom.co.uk/~nineladies/>

---

## ✶ Risks and madness on the BT Cellnet site

"Mike Perry" <PERRYM@uk.ibm.com>

Fri, 24 Aug 2001 18:39:42 +0100

I've just registered with the BT Cellnet site in order to be able to view my mobile phone bill online. I had to choose some authentication items, and I quote here from the website:

```
=====
For security purposes our on-line services are password
protected -- in
```

order to use them you need to register by providing a username, password, a memorable item, and a password hint.

Your Username and Password must be unique to yourself. Try to use something memorable - you will need to use these every time you logon.

Your Password will expire every 90 days and you will be required to choose a new one. You will be automatically prompted to change your password whenever you logon after the 90 day period has expired. To make your password easier to remember you can use the same password but add a different number each time a change is needed. For example password1, password2, password3 and so on.

=====

Looks like a well-known risk is not as widely-known as we might hope.

But wait -- it now leaves the realm of "bad", and enters the "mad":

=====

The Password Hint is a word or phrase that you can choose to remind you of your password should you forget it. For example if your password is your pet's name then the password hint could be 'pet's name'.

The Memorable Item is something that you will need to supply whenever you need to see your Password Hint. Again try use something that is linked to, and therefore will remind you of, your password and password hint.

=====

The usual way that Web sites provide for forgotten passwords is to set up a challenge-response, where the user gives a question that should be asked if they forget their password, and the answer they will give to prove who they are. So you can pick things which you are (fairly) sure wouldn't be known by a miscreant, such as "what's the serial number on the back of your watch?" or "what was the name of your first girl/boyfriend?". This has always seemed to me to be a secure enough system where you don't fear network snooping etc.

But how am I expected to remember "something that is linked to, and therefore will remind you of, your password and password hint" in order to help me when I've forgotten my password?

I know - maybe I'll write it down.....

Mike Perry, IBM UK Webserver Group

---

## **✶ Not such an equal opportunity**

Bill Lamb <blam@wmlc.net>

*Fri, 17 Aug 2001 17:22:30 -0500*

I recently attempted to apply online for a position with Tarrant County College in Fort Worth, Texas.

The first screen in the Web form was for Affirmative Action purposes and required such items as full name, address and Social Security number.

Fortunately, I noticed there was no indication the connection had been secured: no warning from my browser and no "locked" icon in the browser window. I quit the site and e-mailed the school's HR department to report the problem and ask for a "snail mail" address to which to send my resume.

Later that day I received a response from an HR employee stating the school accepts applications only via the online forms, but they are indeed secure. Alternatively, I was welcome to visit the school's library to apply online using one of their machines if I still felt uncomfortable in doing so over the Internet.

I again e-mailed, restating the problem with their supposedly secure connection, and noting that since I lived more than a hundred miles away I wasn't likely to visit the campus simply to fill out a form.

Two days later I received a reply stating a "supervisor" would contact me shortly. That was five days ago. No supervisor yet.

The risks of such a Web connection that may or may not be secure are obvious. But the hidden - and greater - risk here lies in the institution's apparent blind slavery to this new technology. While no doubt making their jobs easier, the policy of only accepting applications online closes off employment opportunities to an untold number of people simply because they may not have access to the Internet or live within bus, car or walking distance of the campus.

Not such an Equal Opportunity Employer, after all, though I know that wasn't their intent.

Bill Lamb    blam@wmlc.net    www.wmlc.net

---

## ✶ Re: Code Red 9? Code Crimson (McDonald, [RISKS-21.62](#))

"Bob Frankston" <rmf2gRisks@bobf.Frankston.com>

*Sat, 25 Aug 2001 19:07:02 -0400*

By this reasoning, one shouldn't buy software from companies that write software in languages that don't make buffer-length checking the norm such as C and it's variants including C++. Languages such as Java, C# and PL/1 don't suffer this unless programmers get too clever and try to squeeze out that extra nanosecond that an indirection may entail. Remember that a computron saved means hours wasted!

[Yes, I know this is a more complicated topic, but a vow of poverty isn't the answer to all problems -- not that I like being put in the position of defending Microsoft.]

---

## ✶ Risks of outsourced check verification

<Peter\_Simpson@ne.3com.com>

*Tue, 14 Aug 2001 07:32:12 -0400*

I recently tried to pay for some clothing with a personal check at a large, national clothing store. I was asked for a driver's license, which I produced, and the sale went through normally.

I then went to a different department, and, again, tried to pay for more clothing with a check. Produced my license. The clerk told me the "transaction had been declined". I asked why, and she handed me a cash register receipt with a code number and an 800 number. I asked her if I could use her phone to call the number (hoping to straighten out whatever the problem was) and was told they could not use it to call outside numbers.

When I got home, I called the number. It was a third party check approval service. The person on the other end of the line asked for my ID (license) number. She then told me that the transaction had been declined because of "unusual check-writing activity". I asked her exactly what that meant. She told me that they had just approved my check number 202 and then tried to use check number 221. The first clerk had transposed two digits while manually entering the check number.

So, my second check was declined. Of course, this "wasn't their fault", and "wasn't the first clerk's fault, either...people make mistakes". My comment that this mistake could easily have been cleared up if I had been allowed to know why the check had been declined fell on deaf and uncaring ears.

I liked it better when the manager was called and scribbled his

initials on  
the check.

Peter Simpson

---

## ✂ Can't hold room, but can bill

Sandy Antunes <sandy@rpg.net>

*Fri, 17 Aug 2001 16:03:58 -0400*

I had a reservation (via phone) with the Hyatt for a trade show. Later I cancelled the credit card used to reserve it, so I called the Hyatt to give them a new card number.

Problem 1: I couldn't find the confirmation number they'd given me.

Problem 2: They couldn't find a reservation for me, and insisted I did not have one. And the hotel was booked for the entire trade show.

Solution (mine): Booked at another hotel.

... time passes ...

I get a statement from the cancelled credit card, listing a charge by the Hyatt for 1 day's stay. Oh oh. I call the Hyatt. The clerk is easily able to call up my record using the credit card number and verify that yes, I had a reservation and yes, I hadn't called to cancel it so I had to pay for 1 night.

Oh, and they'd mistyped my name. Which to me explained why they'd 'lost' my reservation in the first place. He got manager approval to refund the

credit charge because it lacked a "Cancellation Number", and it'll be at least one billing cycle before it goes through.

So they couldn't find my information when I wanted to stay, but could find it to bill.

Risks? Reservation clerks not believing customer, inconsistent procedures and lookups, inaccurate data entry still being accepted by credit card company, cancelled card not rejecting charges, probably others.

Sandy Antunes <aantunes@science.gmu.edu>

---

## **✶ Caller ID vs. ANI confusion, again**

"William Kucharski" <kucharsk@mac.com>

*Sat, 18 Aug 2001 01:50:02 -0600*

In [Risks-21.57](#), Mike Tuffs writes about his credit-card company getting his phone number despite his having Caller ID blocked.

Once again, there are two distinct and COMPLETELY SEPARATE systems that deliver calling phone numbers information to recipients. The system used for toll-free numbers (which the author undoubtedly used to call his credit card company) as well as for long-distance call billing and for 911 services is called ANI.

ANI CANNOT be blocked, at least not without making a significant (and likely questionably legal) effort to thwart the telephone system.

I suspect the answer about ignoring the "ignore" bit is just a script they give the customer service people, or the agent was just making it up.

The bottom line is that your calling number is delivered to the recipient of any toll-free call you make, whether in real time or via a billing statement, REGARDLESS of whether you have Caller ID blocked or not.

William Kucharski <kucharsk@mac.com>

[Noted by quite a few readers, including the following. TNX. PGN]

---

## **✶ Re: Mixing advertising and credit-card activation**

"John Clarke" <jclarke@nortelnetworks.com>

*Fri, 17 Aug 2001 16:44:13 -0400*

[...]

An interesting story, and possibly an urban legend, about ANI. When computerized call centers were becoming the norm, a major credit-card company decided to use ANI to help the operators handle customer calls in a more friendly manner. When a customer called from their home number, the computers would automatically match the number to the account holders name, even before the operator had picked up the call. The operator would then, upon hearing the callers voice, respond with <Mr., Ms.> Account Name, how can I help you?

Callers were so disturbed by the fact that the operator knew who they were before they had identified themselves that the credit-card company eventually told the operators to stop using this technique. They still know who you are (or are likely to be), but withhold the info and allow you to provide it before they use it. Customers are much happier with this method.

When you call an 800 number and reach a call center, your file has likely already appeared on the agent's computer screen, whether they let you know that or not.

---

## **✶ REVIEW: "Information Security Management Handbook", Tipton/Krause**

Rob Slade <rslade@sprint.ca>  
*Mon, 27 Aug 2001 12:08:32 -0800*

BKINSCMH.RVW 20010609

"Information Security Management Handbook", Harold F. Tipton/  
Micki

Krause, 2000, 0-8493-9829-0/0-8493-0800-3, U\$155.00

%E Harold F. Tipton haltip@ix.netcom.com

%E Micki Krause Micki.Krause@isc2.org

%C 2000 Corporate Blvd. NW, Boca Raton, FL 33431

%D 2000

%G 0-8493-9829-0, 0-8493-0800-3

%I Auerbach Publications

%O U\$155.00 800-272-7737 auerbach@wgl.com slinton@crcpress.com

%O available separately 0-8493-9829-0 \$95.00 0-8493-0800-3

\$59.95

%P 2 vol., 711 p. + 626 p.

%T "Information Security Management Handbook, Fourth Edition"

As an overview for the CISSP (Certified Information System Security Professional) CBK (Common Body of Knowledge), this work covers a vast range of topics. The CBK, and the book, is divided into ten domains, covering access control systems, telecommunications, security management, systems development, cryptography, security architecture, operations security, business continuity, law and ethics, and physical security. The text provides some excellent articles, some of which are general but detailed overviews, and others that address particular problems or new technologies. However, even with fifty nine articles and over thirteen hundred pages there are gaps, some surprisingly basic.

The quality of the articles can vary widely. The first essay, on biometrics, provides an admirable review of the subject, as well as some solid, practical, and useful detail information. The next paper is a rather odd treatment of single sign-on, addressing the concepts well, but in a disjointed manner that makes reading or studying difficult. Following those comes a paper ostensibly dealing with securing connections to external networks. It collates some generic and vague descriptions of a variety of topics, none of which are particularly informative or reliable. (A two-page section on computer viruses contains numerous glaring and significant errors. Personally, I continue to find it appalling that general security texts deal so poorly with this topic.)

Other areas covered are firewalls (terse), perimeter security for the Internet (again, but this time with excellent technical information on TCP/IP specifics), extranets (doctrinaire), firewall management (very useful for planning), the OSI (Open Systems Interconnections) network layer security model (questionable utility), the OSI transport layer security model (not much better), application layer security (interesting but undetailed), communications and security protocols (broad overview, concise but fills in some common gaps), security awareness training (reasonable points for success), security architecture (brief but basic), IPsec (good overview), risk analysis (thorough but perhaps a trifle pedantic), trade secret protection (an interesting twist), information security for healthcare (a tad verbose and US-centric), security for object-oriented databases (listing proposals), fundamentals of cryptography (very clear explanations of the math involved), key management (great review of principles, and amusing anecdotes from history of the \*wrong\* ways to manage keys), Kerberos (extensive coverage of both details and concepts), PKI (Public Key Infrastructure, a quick guide to the basics), microcomputer and LAN security (good concepts, overly optimistic, oddities in details), trapping intruders (quick concepts), Java security (quick basics), business continuity planning (a new process), restoration after disaster (general review), computer crime investigation (good coverage of many aspects),

Internet ethics (emphasis on privacy), jurisdictional issues (miscellaneous), intrusion detection (concepts and evaluation points), single sign-on (opinion this time), authentication services (concepts and amusing overview), email security (concept review), ATM (Asynchronous Transfer Mode) security (without really discussing security), remote access (background fundamentals), sniffers (concepts and details), enclaves (firewalls within), IPsec (good details), penetration testing (very basic policies), policy (some good points but quite random), the security business case (opinion), PeopleSoft security (as for any major database), World Wide Web application security (reiteration of general security planning with a few Web specifics), common system design flaws (an important set), data warehouses (standard system development advice with limited security relevance), PKI (simplistic), introduction to encryption (a good one), new models for cryptography application (useful for planning), cryptanalysis (decent review of terminology), message authentication (detailed), UNIX security (concepts and tools), hacker tools (not very detailed), malicious code (theoretical and incomplete), business impact assessment (after Y2K), computer crime investigation (document everything), computer incident response teams (CIRTs, vague), intrusion detection (vague and repetitious), and operational forensics (retain evidence and data).

Observant readers will have noted a fair amount of duplication in that list.

In fact, the reiteration of content is worse than appears here, since many

topics rely on others, and certain basic ideas (Kerberos operations, the Diffie-Hellman public key system, and risk management, for three examples) recur in a variety of other discussions, with differing levels of detail. As in any work this size a number of outright bizarre mistakes have occurred, like the table showing the file structure of an authentication database, which has been swapped with the structural diagram of a completely different authentication system.

This is the closest thing there is to a textbook for the CISSP exam. It is fairly easy to see which sections have been reproduced in the ISC (2) (International Information System Security Certification Consortium) course (in some cases complete down to specific errors). Intriguingly, there are sections of the course that previously were covered by the third edition, and which do not appear in any significant form in this work. (An example is the discussion of the standard formal security models, such as Bell-La Padula and Clark-Wilson.)

It should be noted that there is a significant difference in character between the two volumes. The first volume deals with topics that are closer to the heart of security, and the essays are generally more valuable to the practitioner. Volume two contains papers over a wider range of subjects, many of which (with the notable exception of the pieces on cryptography) have little or no relevance to security beyond fundamental concerns that are well covered elsewhere. Book one will be useful to the CISSP

candidate and  
any specialty security worker: book two may be of interest to a  
narrower  
group of senior security executives and theorists, and,  
ironically, a wider  
audience of those interested in newer technologies in general.

The quantity of good information that is contained in the work is  
definitely worth the price, but there could easily be a wholesale  
pruning of deadwood.

copyright Robert M. Slade, 2001 BKINSCMH.RVW 20010609  
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/  
~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 21: Issue 65**

**Saturday 8 September 2001**

## Contents

- [More about Star Wars 2: "Letter from America"](#)  
[Pete Mellor](#)
- [The Heavens at War: NMD assessed](#)  
[Leonard Erickson](#)
- [Getting the Facts Out - Announcing "FACT SQUAD"](#)  
[Lauren Weinstein](#)
- [Citibank ATM network outage](#)  
[Joshua L. Weinberg](#)
- [France Telecom inadvertent disclosure blamed on "computer error"](#)  
[Peter Campbell](#)
- [Photo tickets dismissed in San Diego](#)  
[Jim Griffith](#)
- [Web filter considered harmful](#)  
[Thomas Roessler](#)
- [Early morning phone call angers citizens](#)  
[Barry Hurwitz](#)
- [New software lets managers search e-mail](#)  
[Jonathan Leffler](#)
- [Consumer Reports password policy risks](#)  
[Bill Bumgarner](#)

- [Norton Personal Firewall](#)  
[Ben Laurie](#)
  - [Solar parking meters are a bad idea in wet Britain](#)  
[David Mediavilla Ezquibela](#)
  - [Sacramento woman denied \\$2.8 million jackpot](#)  
[Max](#)
  - [Accidental disclosure](#)  
[Gene Spafford](#)
  - [Re: Air Force office mails confidential information](#)  
[Maj. John Robinson](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

## ✶ More about Star Wars 2: "Letter from America"

Pete Mellor <pm@csr.city.ac.uk>  
*Sun, 2 Sep 2001 21:11:07 +0100 (BST)*

The following is a summary of Alistair Cooke's "Letter from America" this week (BBC World Service and Radio 4, Sunday 2nd September 2001).

As in my previous message about "The Heavens at War", I have tried to give a fair summary, indicating personal comments by [PM: blah, blah].

Technical Aspects:

Cooke summarised the progress on the National Missile Defense (NMD) project, and referred to the recent successful interception flight test (IFT-6).

He then raised a problem with the vehicle used as a target. After talking about the various technical terms used in defence (going back to the time when journalists had to learn terms like "uranium" and "plutonium") he

introduced the latest term: "spin-stabilisation".

[PM: I downloaded the glossary of terms and acronyms from the Ballistic

Missile Defense Organization's website. It occupies over 800 Kbytes in pdf format.

Follow the link from:

<http://www.acq.osd.mil/bmdo/bmdolink/html/bmdolink.html> ]

An advanced missile such as the USA is capable of launching would use spin-stabilised warheads. Rotating them increases their accuracy, but also makes their trajectory more predictable and so they are easier to track in mid-course than cruder missiles. The targets used in the interception flight tests were spin-stabilised.

Cooke quoted an anonymous source in the DoD who said that he had no illusions about the difficulty of implementing the Star Wars interception system, but having to intercept crude "wobblers" was an enormously difficult task, particularly in the presence of similarly wobbly decoys. The problem is due precisely to the primitive nature of the missiles that are likely to be launched in an attack from a less developed country!

Around 100 acres of US Government land in Alaska have been set aside for testing interceptor flights to hit some of the USA's own crude wobbly rockets. Cooke's source said: "To succeed will take years and years". So, if North Korea can wait until 2004 before launching a rogue attack, the US might be able to intercept it!

Three systems are therefore under development:-

1. To intercept a spin-stabilised warhead,
2. To intercept the "wobbly tumbler" warheads which are still capable of causing massive damage although they might end up miles off target, and
3. (The supreme technical achievement) to detect real from fake wobbly tumblers and hit the right one.

Cooke quoted General Ronald T. Kadish:

Our test philosophy is to add, step-by-step over time, complexity such as countermeasures and operations in increasingly stressful environments. This approach allows us to make timely assessments of the most critical design risk areas. It is a walk-before-you-run, learn-as-you-go development approach. These testing activities provide critical information that reduces developmental risk and improves our confidence that a capability under development is progressing as intended.

[The Ballistic Missile Defense Program. Address by Lieutenant General

Ronald T. Kadish, USAF Director, Ballistic Missile Defense Organization, before the House Armed Services Committee on the Amended Fiscal Year 2002

Budget. July 19, 2001

<http://www.acq.osd.mil/bmdo/bmdolink/html/kadish19jul01.html> ]

(Cooke added a contemptuous "Harrumph".)

The Political Dimension:-

Although journalists are in the habit of saying that the President will do this or that, the budget for any proposal must go through both Houses of Congress before it is passed and funds become available. (The

President  
proposes, Congress disposes.)

A further question is: Does the President have the constitutional right to abrogate the ABM treaty?

A 2/3 majority in Congress is required to empower the President to sign a treaty.

In 1978 the late Senator Barry Goldwater brought suit against President Jimmy Carter to prevent him withdrawing from the Mutual Defence Treaty with Taiwan. The Supreme Court ruled 6 to 2 in Carter's favour, and stated in its judgment that such a decision is down to the executive and branches or the legislature.

A senior constitutional lawyer has stated that the Senate should decide next week after its summer recess if the President does have that power. If the Goldwater/Carter case is taken as a precedent, then the President could in theory opt out of any or all treaties to which the US is party (including withdrawing from the United Nations and NATO!)

Cooke concluded that, all things considered, including the probable cost [PM: \$7,044.779 million for fiscal year 2002 alone, from Kadish's address] and the serious doubts about the constitutional right to abrogate the ABM treaty, "The prospect for Star Wars 2 seems, to put it mildly, ill-starred!"

[PM: Footnote. See slide 13 in the news briefing on the interceptor flight test:-

<http://www.defenselink.mil/news/Aug2001/g010809-D-6570C.html>

Several software problems interfered with the functioning of the ground tracking station.]

Peter Mellor, Centre for Software Reliability, City University, Northampton Square, London EC1V 0HB +44 (0)20 7040 8422 <p.mellor@csr.city.ac.uk>

---

## **✶ The Heavens at War: NMD assessed**

Leonard Erickson <shadow@krypton.rain.com>

*Sun, 2 Sep 2001 05:31:10 PST*

I'm just going to point out a few examples of a major risk here, the arguments being advanced as to possible counter-measures against lasers show a *\*fundamental\** misunderstanding of the means by which weapons lasers damage targets.

They don't *\*burn\** thru the surface, they deposit *\*huge\** amounts of energy (kilojoules to megajoules) into the surface layers of the target in *\*microseconds\**.

The time scale makes rotating the vehicle a bad joke. And the energy levels make reflective coatings an equally bad joke.

At these energy levels, the target spot *\*explodes\** into plasma with effect equivalent to a fair sized chunk of TNT.

And this has pointed out back when SDI was being worked on. Yet these  
\*same\* "problems" are still being pointed out.

There are similarly disingenuous aspects to the discussion of decoys.

Given that none of this appears to have been mentioned in the program,  
I have to conclude that it wasn't even \*remotely\* objective in assessing  
the missile defense program.

In short, from what was reported to RISKS, the program was badly slanted. And hardly anything to base a risk evaluation on.

Other aspects of the post make it seem inappropriate for RISKS as well.

As a counter, let me just note that there are risks to \*not\* trying to  
develop a defense. And to spreading grossly inaccurate "risk assessments" regarding something that is in it's early testing stages.

There are potential problems. But bringing up "problems" like the ones  
I mention above is not eliminating risks, it's spreading propaganda.

Other items brought up may be valid risks or invalid ones, depending on  
one's assessment of the relative risks of no missile defense versus one that  
is not 100% effective. But \*that\* aspect of things is \*not\* a valid topic  
for \*this\* list! Not unless there's been a major policy change that I'm  
unaware of.

Leonard Erickson (aka shadow{G}) shadow@krypton.rain.com

## ✂ Getting the Facts Out - Announcing "FACT SQUAD"

PFIR - People For Internet Responsibility <pfir@pfir.org>

Thu, 6 Sep 2001 19:26:50 -0700 (PDT)

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

[ To subscribe or unsubscribe to/from this list, please send the command "subscribe" or "unsubscribe" respectively (without the quotes) in the body of an e-mail to "pfir-request@pfir.org". ]

Getting the Facts Out - Announcing "FACT SQUAD"

September 6, 2001

<http://www.pfir.org/factsquad-announce>

Greetings. Immediately following the recent People For Internet Responsibility "Future of the Internet" Workshop, technology columnist Dan Gillmor reported on the event within his widely-read column. He especially noted one of the key points of agreement at the meeting -- there's a serious need for coordinated information sources and experts to counter the often skewed information provided by lobbyists and other vested interests relating to technology issues. As it stands, it's usually those well-heeled interests who have successfully organized, for their own betterment, to provide information about technical matters to media, politicians, and many others.

Dan used the term "fact squad" to describe the need for a coordinated effort

to provide some balance in these matters.

PFIR has now set up a structure that we hope can provide assistance in filling this fact gap. We've created "Fact Squad" -- its home page, which describes the project in more detail, is at:

<http://www.factsquad.org>

Fact Squad is oriented specifically towards folks who need straightforward, direct, and largely "jargon-free" information about these topics. It is a coordinated resource for media, researchers, or anyone else -- cutting through the hype and getting to the facts.

Fact Squad by itself obviously cannot be the complete solution to the long-festering and worsening problems of manipulated information and propaganda relating to technical issues and their impact on society. But we think it's potentially an important step in the right direction.

In addition to the Fact Squad home page listed above, three new contact e-mail addresses have been established relating to this effort:

- Questions or information about specific topics or issues:  
facts@factsquad.org
- General inquiries:  
general@factsquad.org
- Information about participating in Fact Squad:  
participate@factsquad.org

We look forward to your questions, comments, and participation.

Thanks very much.

Lauren Weinstein

lauren@pfir.org or lauren@vortex.com or lauren@privacyforum.org  
Tel: +1 (818) 225-2800  
Co-Founder, PFIR - People For Internet Responsibility - <http://www.pfir.org>  
Moderator, PRIVACY Forum - <http://www.vortex.com>  
Member, ACM Committee on Computers and Public Policy

Peter G. Neumann  
neumann@pfir.org or neumann@csl.sri.com or neumann@risks.org  
Tel: +1 (650) 859-2375  
Co-Founder, PFIR - People For Internet Responsibility - <http://www.pfir.org>  
Moderator, RISKS Forum - <http://catless.ncl.ac.uk/Risks>  
Chairman, ACM Committee on Computers and Public Policy  
<http://www.csl.sri.com/neumann>

---

## **⚡ Citibank ATM network outage**

"Joshua L. Weinberg" <joshua@theWeinbergs.com>  
*Wed, 05 Sep 2001 09:16:25 -0700*

Citibank's network of 2000 automated teller machines went down on the evening of 4 Sep 2001, due to software problems. It was still down the next day. Citibank's online Internet system also crashed at the same time.

Basic service was restored about two hours later, but various problems persisted. [Source: Reuters item, 5 Sep 2001; PGN-ed]

[http://dailynews.yahoo.com/h/nm/20010905/bs/financial\\_citibank\\_dc\\_2.html](http://dailynews.yahoo.com/h/nm/20010905/bs/financial_citibank_dc_2.html)

Joshua L. Weinberg, 2 Townsend St., Apt 1-905, San Francisco, CA 94107  
1-415-777-3339 joshua@theWeinbergs.com

---

## ✦ France Telecom inadvertent disclosure blamed on "computer error"

"Peter Campbell" <peter.a.campbell@worldnet.att.net>

Thu, 6 Sep 2001 20:28:19 -0500

A variant on the risk of leaving information you don't want disclosed in 'comments' part of a MS Office document, except that instead of the consequences being just egg-on-face, there are selective disclosure issues and the potential for accusations of unfairness. In the US, class action lawsuits have been attempted for less.

<http://public.wsj.com/sn/y/SB999174259870751856.html>

<http://biz.yahoo.com/prnews/010830/nyth052.html>

For the uninitiated, selective disclosure of material information is a mortal sin in the investment world. The underlying principle of financial markets is one of fairness to all shareholders -- stock in a company is not called "equity" for nothing. Executing trades based on information to which all shareholders do not have access is called insider trading, though mechanisms do exist that allow insiders to trade in a perfectly legitimate and legal fashion, and is a grave offense in most countries with developed financial markets. Of course, most large investors have more time, resources and expertise to devote to decision making than most small ones, so their advantage is undeniable. But the basis for making investment

decisions, so-called material information, must be available to all investors, large and small. A widely discussed regulation, dubbed Reg FD (for Fair Disclosure) was adopted by the SEC in October of 2000: more information on that here:

<http://www.sec.gov/rules/final/33-7881.htm>

Back to the subject and the risk: the error is obviously human and the risks of email compounded with the notes/comments/change-tracking features have been discussed many times in Risks. Indeed the company I work for released a PR document with the revision history intact... I can happen to the best of us !

---

## **✶ Photo tickets dismissed in San Diego**

Jim Griffith <[griffith@olagrande.net](mailto:griffith@olagrande.net)>  
*Tue, 4 Sep 2001 18:22:57 -0500 (CDT)*

A judge in San Diego dismissed 290 tickets issued by a new red light camera system. The issue was a \$70 contingency fee paid per ticket to the private company operating the system, which gave that company a clear monetary incentive to issue more tickets. The case in question may impact the fifty other cities in the nation which also use red light camera systems. The judge did not question the accuracy of the technology itself.

[http://abcnews.go.com/wire/US/reuters20010904\\_522.html](http://abcnews.go.com/wire/US/reuters20010904_522.html)

## ⚡ Web filter considered harmful

Thomas Roessler <roessler@does-not-exist.org>

*Fri, 7 Sep 2001 12:42:11 +0200*

Today, I had to call Palm Support Germany about some problems encountered with one of their new models (insert m500 into the USB cradle, and the PC will occasionally reboot).

The call-center guy I had on the phone hadn't heard about the problem.

However, I had done a web search before, and had found some mailing list discussions where someone reported that Palm's US second-tier support knew the problem quite well.

So I gave the list archive's URL to the guy, asking that he investigates the problem.

"Sorry, I can't access this through our web proxy. They want to be sure that we don't surf for private purposes during work hours."

The RISK should be obvious: Filtering support employees' web access for security or whatever other reasons can seriously damage these employees' ability to do their job.

Thomas Roessler  
[org/](http://log.does-not-exist.org/)

<http://log.does-not-exist.org/>

---

## **⚡ Early morning phone call angers citizens**

"Barry in Indy" <barryindy@ameritech.net>

*Sun, 2 Sep 2001 06:49:52 -0500*

A lightning strike caused a computer to begin sending out an automated phone message in the middle of the night. The meeting announcement, scheduled to be delivered during the day on Friday, August 31, but was sent starting after 9 PM Thursday night, and continued until 3:30 AM Friday. There were about 50 complaints.

<http://www.indystar.com/print/citystate/sat/articles/badcall01.html>

The RISKS? Political suicide, at the least.

Barry Hurwitz

---

## **⚡ New software lets managers search e-mail**

Jonathan Leffler <jleffler@informix.com>

*Wed, 5 Sep 2001 12:49:04 -0700 (PDT)*

Note from \*Computerworld\*: Managers everywhere will soon have the power to remotely check employee e-mail boxes, search for common words and even delete e-mail without notification, thanks to new software.

[http://computerworld.com/nlt/0%2C3590%2CNAV47\\_STO63417\\_NLTDM%2C00.html](http://computerworld.com/nlt/0%2C3590%2CNAV47_STO63417_NLTDM%2C00.html)

[JL: The risks of abuse seem legion. And accidental abuse could

occur;

what if that deleted email was actually important?]

Jonathan Leffler (Jonathan.Leffler@Informix.com)

Guardian of DBD::Informix v1.00.PC1 -- <http://www.perl.com/CPAN>

---

## **✶ Consumer Reports password policy risks**

Bill Bumgarner <bbum@codefab.com>

*Wed, 05 Sep 2001 17:40:57 -0400*

My family regularly uses \*Consumer Reports\* to evaluate various products before we make a purchasing decision.

The enclosed e-mail is the culmination of a rather round-about discussion.

The original problem was that I could not log into my CR account [paid subscription] because it kept claiming the password is incorrect. Eventually, I discovered that I could log in if I claimed that I had forgotten my password and forced the site to send me a "click here to change your password" URL via email (in plain text, of course).

Along the click trail of "click here to change your password", the user enters a new password twice, verifies the two passwords matches, logs the user in (to the edit the account page-- ugh), and presents the user with the site as if they had successfully logged in.

If the user happens to choose a password containing an exclamation point (!), the site silently drops the exclamation point without giving the user

any feedback that it has done so. Subsequent login attempts, of course, fail (unless the user happens to forget to type the (!)).

Risk #1: Silently modifying the user's entered password, claiming successful entry, and storing the modified (and likely insecure password)

Risk #2: Limiting passwords to just letters/numbers. Most good password crackers will brute force through all the various 'dog', 'd0g', d)g' possibilities.

Risk #3: Having a "forgot your password" click path that leads directly to all of the pertinent account information. Thankfully, it does not display your FULL credit card-- but does give the last five digits and does allow the user to modify various bits of critical information.

Risk #4: Sending the "forgot your password" URL in a plain text email. A dead horse.

Risk #5: Having nice, responsive customer support that had \*no clue\* that this problem existed (or even that it was a problem) when, in fact, the problem has been an issue for nearly a year (maybe longer).

I'm sure there are others...

b.bum

(enjoying a 'Fisher & Paykel' as a result of information found on the above site.... talk about killer engineering. Drop a couple of wet sneakers in it, set it to spin dry at 7,000 RPM and it actually balances the drum to keep the thing from tearing itself apart!)

Begin forwarded message:

> From: customerservice@customerrelations.consumer.org  
> Date: Wed Sep 05, 2001 05:14:24 PM America/Montreal  
> To: "Mr. Bill Bumgarner" <bbum@codefab.com>  
> Subject: Message from Consumer Reports Online - Ref:382442  
>  
> Dear Mr. Bumgarner:  
>  
> Thank you for your recent e-mail. It was a pleasure to hear  
from you.  
>  
> After reading your e-mail, I'm sorry to say that your password  
cannot have  
> an exclamation point (!). However, please be assured that  
your password  
> can indeed consist of letters and numbers. If you have any  
questions,  
> please feel free to contact our Online Subscription Department  
toll-free  
> at  
> (800) 633-0663. A representative will be more than happy to  
assist you.  
>  
> Again, thanks for your e-mail. I hope you continue to enjoy  
the benefits  
> of Consumer Reports OnlineÆ.  
>  
> Sincerely,  
>  
> Jenny Manzueta  
> Customer Relations  
> 382442

In cyberspace, no one can hear you laugh.

---

 **Norton Personal Firewall**

Ben Laurie <ben@algroup.co.uk>  
*Tue, 04 Sep 2001 20:31:08 +0100*

I recently had a problem with a Web site I run. A user complained that Norton Personal Firewall was saying the site was "trying to access her bank account details". Much investigation later, we discovered that the problem was completely stupid.

NPF protects the user from sites that allow them to enter sensitive information in a form that is not secured by SSL. I guess there's some value in this. However, a number of factors combine to produce completely unnecessary FUD, not to mention a complete waste of everyone's time.

Firstly, users are advised to protect their credit/debit card numbers by entering only some of the digits - the recommended number being 4.

Secondly, the "firewall" objects to a web page being served by the server containing the sensitive information if the page contains a form and is not secured by SSL. However, it does not check whether the data presented is even in the form.

Thirdly, the message presented to the user suggests that the webserver is somehow trying to access the sensitive data rather than present it (I'm afraid I do not have the exact wording - figuring out the problem was tedious enough without trying to elicit such details from the user).

The net effect of all this is that you get hysterical messages from the user

(and everyone else on the mailing list they post this problem to) saying that you are trying to steal their credit card numbers.

And the cause? A link containing a timestamp in seconds. For any 4 digit sequence the timestamp will match it for 1 second approximately 10 times a day, for 10 seconds once a day, for 100 seconds every 10 days, and so on. This lucky user happened to have a number that recently matched all the time for a period of 12 days.

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

---

## **⚡ Solar parking meters are a bad idea in wet Britain**

<David Mediavilla Ezquibela>  
*Thu, 6 Sep 2001 20:26:55 +0200*

<http://news.telegraph.co.uk/news/main.jhtml?xml=/news/2001/09/06/nmet06.xml>

Nottingham Council (United Kingdom) admitted that the 215 parking meters powered by solar energy that they installed didn't function as expected. They followed the example of other countries in sunny Southern Europe, but, even when this summer has been sunnier in Nottingham, several meters have failed allowing parking for free during periods. Others didn't work even in sunshine because they were under trees. The provider, Metric, is adjusting them for winter to save energy.

David Mediavilla Ezquibela

<davidme.forum@bigfootNO.SPAMcom>

---

## ✶ Sacramento woman denied \$2.8 million jackpot

Max <max7531@earthlink.net>

*Fri, 07 Sep 2001 15:28:16 -0700*

[The RISK: having a failure mode the same as the winning mode. Max]

Nevada Gaming Control Board agents say a Sacramento woman did not win a \$2.8 million jackpot she thought she won last month at a Reno casino because the machine malfunctioned. "The first reel started to spin, and it touched a maintenance card," said Paul Dix, a Gaming Control Board supervisor. "And the machine did what it was supposed to do. It went into a tilt." But Francesca Galea, 29, insists her play was a legitimate win. And she's willing to fight for the winnings. [PGN-excerpted from AP report, 7 Sep 2001]

---

## ✶ Accidental disclosure

Gene Spafford <spaf@cerias.purdue.edu>

*Wed, 5 Sep 2001 08:42:03 -0500*

Several recent Risks Digests have (once again) illustrated hazards associated with accidental disclosure of personal information online.

Readers who do not get the Computing Research Association News might want to check the May issue. I wrote a cautionary article about using online applications and recommendation letter collection, specifically for academia.

See <<http://www.cra.org/CRN/issues/0103.pdf>> for " Protecting Personal Information in Academia."

---

## **✶ Re: Air Force office mails confidential information ([RISKS-21.63](#))**

<tympani@att.net>

*Wed, 05 Sep 2001 14:53:18 +0000*

Re: the USAF Academy e-mail foul-up mentioned in [RISKS-21.63](#):  
the standard  
e-mail package for Air Force offices is MS Outlook, which lets  
you assemble  
lists of names into addressee groups to avoid the hassle of  
typing or  
reselecting a large list of names each time you want to send out  
a mass  
message. What likely happened here is that the officer  
responsible simply  
clicked the wrong addressee group in haste or carelessness; for  
instance,  
instead of selecting "Cadet Group Headquarters" he might have  
selected  
"Cadet Group," which would shotgun the message out to everybody.

Of course there are any number of other ways this could have  
happened, but I  
doubt that there are any shenanigans going on.

Maj. John Robinson, USAF

[Still, it could be SirCam. 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 21: Issue 66**

**Monday 17 September 2001**

## Contents

- [11 September 2001 in retrospect](#)  
[PGN](#)
- [Info on RISKS \(comp.risks\)](#)

## ★ 11 September 2001 in retrospect

"Peter G. Neumann" <neumann@CSL.sri.com>  
*Mon, 17 Sep 2001 16:27:43 PDT*

```

*****
*****
**           11 September 2001           **
*****
*****

```

"THE RISKS ARE OBVIOUS."  
BUT PERHAPS NOT OBVIOUS ENOUGH.

11 September 2001 will be painfully remembered by most of the

planet's population for the coordinated hijacking of four jetliners and the ensuing surprise attacks on New York City's World Trade Center and the Pentagon, with thousands of lives lost and enormous consequential after-effects. Our hearts go out to everyone close to those who were so irrevocably affected -- including the crash victims, the firemen and other emergency workers in New York City, and especially the UA93 passengers whose efforts evidently saved the lives of others.

We are once again reminded how fragile our lives and civic infrastructures are, and how interdependent we all are. Although violent and sudden large-scale termination of people's lives has previously been all too familiar in many countries of the world, many of us have hitherto largely taken too much for granted. Hopefully, the aftermath of this fateful day will dramatically increase public awareness of some of the vulnerabilities in our lives and risks to our freedom.

However, the events should come as no surprise, because many warnings have been widely ignored. For example, the President's Commission on Critical Infrastructure Protection of the previous U.S. Administration identified serious vulnerabilities in telecommunications, electric power and other energy sources, transportation, financial services, emergency services, and government continuity. It noted how interdependent these critical infrastructures are, and how they are all related to information technologies. It also observed difficulties in coordination

among and within different infrastructures, and perhaps most relevant, a general lack of public awareness. In many respects, complacency has been seen across the board in response to that report. In addition, the White House Commission on Safety and Security (the Gore Commission) identified many serious risks in aviation. (Also, see my paper <<http://www.csl.sri.com/neumann/air.html>>, presented at the January 1997 International Conference on Aviation Safety and Security, co-sponsored by that commission and George Washington University.) Various analyses of commercial aviation and air-traffic control over the past 18 years within the Department of Transportation have identified potentially serious vulnerabilities that merit closer attention. More recently, a U.S. General Accounting Office report identified many serious problems in airport security. But, perhaps because the risks and threat levels seemed low, or possibly because institutional bureaucracy is so deeply entrenched, very little action was deemed necessary. Unfortunately, some of the issues recognized therein have now come home to roost.

As a society, we in the U.S. seem to be unwilling to take certain prudent precautions -- perhaps because they would cost too much, or be too inconvenient, or would seriously degrade service. Apparently, we suffer from a serious lack of foresight.

The Risks Forum has persistently considered risks associated with our technologies and their uses, but we often note that many of the

crises and other risk-related problems have resulted from low-tech events, misguided human behavior, or malicious misbehavior. In short, the typical search for high-tech solutions to problems stemming from social, economic, and geopolitical causes has frequently ignored more basic issues. Over-endowing high-tech solutions is riskful in the absence of adequate understanding of the limitations of the technology and the frailties and perversities of human nature. Whereas there are high-tech solutions that might be effective if properly used, we should also be examining some low-tech and no-tech approaches.

One pervasive theme in the Risks Forum over the past 16 years has been the ubiquity of systemic vulnerabilities relating to security, reliability, availability, and overall survivability, with respect to human enterprises, society at large, and to systems, applications, and enterprises based on information technologies. Evidently, we still have much to learn.

Let us seek to build a better world, and remain true to our human values and constitutional foundations. Also, let us beware of seeming solutions -- technological or otherwise -- that result in further escalation of the risks. Sadly, because of the inherent vulnerabilities in those seeming solutions, we are always at risk, whether we realize it or not.

Peter G. Neumann



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 21: Issue 67**

**Monday 1 October 2001**

## Contents

- [Aftermath of 11 September 2001](#)  
[PGN](#)
- [GAO reports on terrorism](#)  
[Monty Solomon](#)
- [Warding off cyberterrorist attacks](#)  
[NewsScan](#)
- [Hackers face life imprisonment under 'Anti-Terrorism' Act](#)  
[Monty Solomon](#)
- [Gartner "Nimda Worm shows you can't always patch fast enough"](#)  
[Alistair McDonald](#)
- [Hacker re-writes Yahoo! news stories](#)  
[Gary Stock](#)
- [YAHA: Yet Another Hotmail Attack](#)  
[Alistair McDonald](#)
- [Hackers and others win big in Net casino attacks](#)  
[Ken Nitz](#)
- [Creator of Kournikova virus gets 150 hours of community service](#)  
[Abigail](#)
- ["Good Samaritan" hacker pleads guilty to breaking and entering](#)  
[Declan McCullagh](#)

- [U.S. court shuts down deceptive Web sites](#)  
[Jim Griffith](#)
  - [Report on vulnerabilities of GPS](#)  
[Joseph Bergin](#)
  - [All public hospitals in Gothenburg Sweden Crippled by nimda](#)  
[Peter Håkanson](#)
  - [Y2K flaw blamed for Down's Syndrome test errors](#)  
[Les Weston](#)
  - [Re: Oxygen tank kills MRI exam subject](#)  
[PGN](#)
  - [E-voting in Australia](#)  
[Tony Jones](#)
  - [Australians voice anger over online spying](#)  
[Monty Solomon](#)
  - [World Trade Center in RISKS](#)  
[Jay R. Ashworth](#)
  - [We only reveal a few digits of your account number, don't worry](#)  
[Dan Jacobson](#)
  - [X-ray machine risk](#)  
[Asa Bour](#)
  - [Increasing RISKS of UPPER CASE](#)  
[Stuart Prescott](#)
  - [2002 USENIX Annual Technical Conference - Call for papers](#)  
[Ann Tsai](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

## ✶ **Aftermath of 11 September 2001**

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

*Mon, 1 Oct 2001 11:06:12 PDT*

The Risks Forum has long advocated the importance of increased awareness of risks and avoidance of critical systems with too many inherent weak links.

On 11 Sep 2001, the Internet stood up well and was a very important source of information; land-based and cellular telephone systems experienced major outages in lower Manhattan. A few companies such as Cantor-Fitzgerald and eSpeed suffered huge personnel losses, but were nevertheless able to resume operations quickly -- through various combinations of advanced planning and rapid recovery strategies. There are many lessons that are worth recording here, so I would like to invite some of you to contribute short but pithy items on what was achieved, what was learned, and what insights you might have gained. [Thanks to Scott Rainey for encouraging me to do this.]

---

## **GAO reports on terrorism**

"monty solomon" <monty@roscom.com>  
*Thu, 20 Sep 2001 17:28:02 -0400*

Combating Terrorism: Selected Challenges and Related Recommendations. GAO-01-822, September 20.

<http://www.gao.gov/new.items/d01822.pdf>

Aviation Security: Terrorist Acts Demand Urgent Need to Improve Security at the Nation's Airports, by Gerald L. Dillingham, director, physical infrastructure issues, before the Senate Committee on Commerce, Science, and Transportation. GAO-01-1162T, September 20.

<http://www.gao.gov/new.items/d011162t.pdf>

Aviation Security: Terrorist Acts Illustrate Severe Weaknesses

in Aviation Security, by Gerald L. Dillingham, director, physical infrastructure, before a joint hearing of the Senate and House Appropriations Subcommittees on Transportation and Related Agencies. GAO-01-1166T, September 20. <http://www.gao.gov/new.items/d011166t.pdf>

---

## 🔥 Warding off cyberterrorist attacks

"NewsScan" <newsscan@newsscan.com>

*Mon, 01 Oct 2001 08:19:36 -0700*

Internet experts believe that the threat of cyber-attacks are increasing, though not necessarily from Osama bin Laden's AlQaida network, which seems focused on destroying physical targets and killing civilians. Georgetown University computer science professor Dorothy Denning says, "It's my understanding that they're not teaching this in the terrorist-training camps," but rather that the danger comes from "these thousands of affiliates or sympathizers." Stephen Northcutt, who runs an information warfare simulation for the SANS Institute, warns that terrorist could "potentially paralyze commerce" and might be able to "accomplish a cascading failure of the electronic grid." (\*San Jose Mercury News\*, 1 Oct 2001; NewsScan Daily, 1 October 2001; <http://www.siliconvalley.com/docs/news/depth/cyber100101.htm>)

[Also, there is clearly renewed interest in off-site backup data storage.

PGN]

---

## **✶ Hackers face life imprisonment under 'Anti-Terrorism' Act**

Monty Solomon <monty@roscom.com>

*Tue, 25 Sep 2001 16:32:58 -0400*

Hackers face life imprisonment under 'Anti-Terrorism' Act;  
Justice

Department proposal classifies most computer crimes as acts of  
terrorism

By Kevin Poulsen, 23 Sep 2001

Hackers, virus-writers and web site defacers would face life  
imprisonment

without the possibility of parole under legislation proposed by  
the Bush

Administration that would classify most computer crimes [and  
maybe noncrimes

(PGN)?] as acts of terrorism. The Justice Department is urging  
Congress to

quickly approve its Anti-Terrorism Act (ATA), a twenty-five page  
proposal

that would expand the government's legal powers to conduct  
electronic

surveillance, access business records, and detain suspected  
terrorists.

[See <http://www.securityfocus.com/news/257> for the full item.

PGN]

---

## **✶ Gartner "Nimda Worm shows you can't always patch fast enough"**

Alistair McDonald <alistair@bacchusconsultancy.com>

*Fri, 21 Sep 2001 13:07:00 +0100*

Gartner is recommending that IIS users who have been hit by the recent MS exploits should "immediately" consider moving to alternatives such as Apache or iPlanet. [http://www4.gartner.com/DisplayDocument?doc\\_cd=101034](http://www4.gartner.com/DisplayDocument?doc_cd=101034)

But when will those in control take note? I'm sure that a lot of NT/2000 sysadmins (and especially Webmasters) are aware of the limitations of their platform, but corporate strategy means that they are a "Microsoft shop".

Alistair McDonald                      Bacchus Consultancy                      www.  
bacchusconsultancy.com

---

## **⚡ Hacker re-writes Yahoo! news stories**

Gary Stock <gstock@nexcerpt.com>  
*Mon, 24 Sep 2001 09:50:34 -0400*

Will Knight, New Scientist, 20 Sep 01  
<http://www.newscientist.com/news/news.jsp?id=ns99991329>

A computer security expert has revealed how he altered news articles posted to Yahoo!'s web site without permission. The incident highlights the danger of hackers posting misleading information to respected news outlets. Freelance security consultant Adrian Lamo demonstrated that, armed only with an ordinary Internet browser, he could access the content management system used by Yahoo!'s staff use to upload daily news. He added the

false quotes  
to stories to prove the hole was real to computer specialist  
site Security  
Focus. Yahoo! has issued a statement saying the vulnerability  
has been  
fixed and security is being reviewed. But experts say that the  
incident  
demonstrates a serious risk. "Just think how much damage you  
could do by  
changing the quarterly results of a company in a story," says J  
J Gray, a  
consultant with computer consultants @Stake.

Gary Stock, CIO & Technical Compass, Nexcerpt, Inc. 1-  
616.226.9550  
gstock@nexcerpt.com

---

## **YAHA: Yet Another Hotmail Attack**

Alistair McDonald <alistair@bacchusconsultancy.com>

*Fri, 21 Sep 2001 09:49:00 +0100*

Yet another attack on hotmail. Computing (20 Sept 2001) reports  
that one can  
hack the hotmail web site, and redirect users to another site.  
This brings  
up the possibility of password collecting. The hacker, known as  
"Oblivion",  
reported this to the bugtraq mailing list. The exploit involves  
smuggling  
javascript code through the filters used at hotmail.

Alistair McDonald                      Bacchus Consultancy                      www.  
bacchusconsultancy.com

## **✶ Hackers and others win big in Net casino attacks**

Ken Nitz <nitz@SDL.sri.com>

Mon, 10 Sep 2001 09:14:27 -0700

<http://news.excite.com/news/r/010910/11/net-tech-gambling-hacking-dc>

[The article is on risks in on-line gambling, and particularly CryptoLogic, Inc., a Canadian on-line casino games developer that has been

hacked. One of their sites had been "fixed" so that craps and video slot

players could not lose, with winnings totalling \$1.9 million. Every dice

throw turned up doubles, and every slot spin generated a perfect match.

Whether it was an insider attack or a penetration is not clear from the

article. (We noted the likelihood of hacking of Internet gambling sites

in [RISKS-19.27](#), 1 Aug 1997, not to mention my 1995 April Fool's piece in

[RISKS-17.02](#).) Interesting question: which laws against hacking will apply

to subversions of illegal Internet gambling parlors? Who gets to

prosecute remote attacks on off-shore operations? PGN-ed]

---

## **✶ Creator of Kournikova virus gets 150 hours of community service**

"Abigail" <abigail@foad.org>

Fri, 28 Sep 2001 01:16:42 +0200

>From <http://www.volkskrant.nl/nieuws/nieuwemedia/1001567916953.>

[html](#)

(in Dutch).

27 Sep 2001

The 20-year-old creator for the Kournikova virus, J. de W. from Sneek, was sentenced to 150 hours of community service by the court of Leeuwarden this Thursday. The prosecution demanded the maximum of 240 hours of community service. In February De W. released on the Internet the so-called wormvirus, which spread itself as an e-mail message. The virus was activated by clicking the e-mail which was titled Anna Kournikova (the tennis player). This lead to inconvenience of Internet users all over the world. When determining the sentence, the court took into consideration that the boy had no previous run-in with justice, that he turned himself in, and that material damages were limited. The American investigation service FBI reported an amount of \$166.827 in damages.

---

## **✶FC: "Good Samaritan" hacker pleads guilty to breaking and entering**

Declan McCullagh <declan@well.com>

*Thu, 27 Sep 2001 12:53:53 -0400*

[Follow-up on [RISKS-21.62](#) items. PGN]

'Good Sam' Hacker 'Fesses Up, By Declan McCullagh, 27 Sep 2001  
declan@wired.com

It seemed like such a straightforward example of prosecutorial misconduct:

An Oklahoma man was being investigated by the Justice Department for helping a newspaper fix a Web site security hole.

The outcry among the geek community last month began with an uncritical story on LinuxFreak.org entitled "Cyber Citizen Lands Felony Charges?" Sites such as Slashdot soon picked up the sad tale of 24-year-old Brian K. West as evidence of out-of-control, tech-clueless government lawyers, and urged everyone to e-mail the U.S. Attorney in charge of the prosecution.

Making the story even more appealing to the open-source community was the Microsoft angle: West was said to have reported to the Poteau (Oklahoma) Daily News and Sun a security flaw in Microsoft NT 4.0 IIS and Microsoft FrontPage. But a guilty plea that West signed tells a far different story -- and shows how easily a well-meaning community of programmers and system administrators can be led astray.

<http://www.wired.com/news/politics/0,1283,47146,00.html>

[Politech archive on U.S. v. Brian K. West:

<http://www.politechbot.com/cgi-bin/politech.cgi?name=sperling>]

[PGN-excerpted from the Sperling release:

While probing the site, defendant made copies of six proprietary

Practical Extraction Report Language (PERL) scripts that were part of

the source code running the PDNS Web page. Defendant also obtained

password files from PDNS and used those passwords to access other parts

of the PDNS Web page. Defendant electronically shared the scripts and

the password files for the PDNS Webs ite with another individual.

Defendant's access to the Web page involved interstate communications.

...]

---

## **⚡ U.S. court shuts down deceptive Web sites**

<griffith@olagrande.net>

*Mon, 1 Oct 2001 14:59:23 -0500 (CDT)*

Reuters reports that the U.S. District Court in Philadelphia has ordered

John Zuccarina to shut down sites operated by him. The Federal Trade

Commission filed a complaint against Zuccarina, claiming that he has

purchased domain names which are misspellings or other "one-offs" of

popular sites, which he uses to "blitz" unsuspecting visitors with pop-up

ads, from which the user cannot escape, in order to receive advertising

revenue (estimated between \$800K and \$1 million). Zuccarina has registered

some 5500 domains, including [www.annakurnikova.com](http://www.annakurnikova.com), 41 variants of

"Britney Spears", and others.

<http://www0.mercurycenter.com/breaking/docs/081329.htm>

---

## **⚡ Report on vulnerabilities of GPS**

Joseph Bergin <berginf@pace.edu>

Tue, 11 Sep 2001 07:31:31 -0400

Yesterday (10 Sept. 2001) the U.S. Transportation dept released a report on the vulnerabilities of the Global Positioning System. The report can be obtained from

<http://www.navcen.uscg.gov/gps/geninfo/pressrelease.htm>

There is a short story about it in \*The New York Times 11 Sep 2001:

<http://www.nytimes.com/2001/09/11/national/11NAVI.html>

The report notes that GPS is being increasingly relied on for life-critical performance in transportation and recommends that various backups be maintained and new ones developed.

Joseph Bergin, Professor, Pace University, Computer Science, One Pace Plaza,

NY NY 10038 [berginf@pace.edu](mailto:berginf@pace.edu) HOMEPAGE <http://csis.pace.edu/~bergin/>

---

## ✶ All public hospitals in Gothenburg Sweden Crippled by nimda

Peter Håkanson <peter@ipsec.nu>

Tue, 25 Sep 2001 10:42:55 +0200

The hospitals in "Västra Götaland" sweden (west coast, population 1M) were isolated from Internet during 23 Sep 2001. Some of internal networks had to be partitioned to prevent nimda spreading further. Reservations and computer-based medical records were unavailable. <http://www.>

[vgregion.se](http://vgregion.se)

The fact that a hospital chain has so relaxed security is amazing. It's also amazing that whole organizations are kept hostage of a vendor that's not even cost-effective.

What would happen in case we get a \*real\* threat to security??

Peter Håkanson, IPsec sverige, Bror Nilssons gata 16  
Lundbystrand  
S-417 55 Gothenburg Sweden "Safe by design" +46707328101  
peter@ipsec.nu

---

## ✶ Y2K flaw blamed for Down's Syndrome test errors

Les Weston <trusteemse@mailexpire.com>

*Fri, 14 Sep 2001 13:24:33 +0100*

The Y2K problem is being blamed for incorrect Down's Syndrome results being given to more than 150 pregnant women throughout northern England between January and May last year. As a result, four Down's syndrome pregnancies went undetected. Amongst other factors, the mother's age is used to assess her risk category. Only those in the high-risk category undergo further tests for the syndrome. Staff noticed the strange results coming from the system, but initially thought they was due to a different mix of women being tested.

Full report:

[http://news.bbc.co.uk/hi/english/health/newsid\\_1541000/1541557.](http://news.bbc.co.uk/hi/english/health/newsid_1541000/1541557)

[stm](#)

Les Weston, Quinag-CSL, Edinburgh.

[Also noted by several others. TNX. Overconfidence in the PathLAN

computer was blamed for errors, occurring between 4 Jan and 24 May 2001.

PGN]

---

## ⚡ Re: Oxygen tank kills MRI exam subject ([RISKS-21.55](#))

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

*Sun, 30 Sep 2001 10:44:16 PDT*

Westchester Medical Center was fined \$22,000 for 11 violations related to the death of the 6-year-old boy killed by the magnetically attracted stray oxygen tank carried into the room by a doctor.

<http://www.newsday.com/news/nationworld/wire/sns-ap-mri-death0928sep28.story>

---

## ⚡ E-voting in Australia

Tony Jones <tmj@enternet.com.au>

*Sun, 23 Sep 2001 06:31:10 +1000 (EST)*

On 20 October 2001 there will be an election of members of the Legislative Assembly of the Australian Capital Territory. It is hoped that about 9% of voting will be done using a new electronic voting system.

Further details

are at <<http://www.elections.act.gov.au/Elevote.html>>.

For the electronic system, no independently verifiable copy of a voter's choices will be kept. The selections made by a voter and displayed on the monitor of the voting computer will be, we're led to believe, what go into the duplicated databases for counting.

RISKS readers will be reassured to know that (see <<http://www.elections.act.gov.au/media0104.html>>):

"The new software will be subjected to extensive testing to ensure it is accurate and secure, as well as easy to use. The software will be used on standard computer hardware, that will not be connected to any external networks. The system will also include numerous backups and safeguards to ensure that voting data will not be lost. This will guarantee the security of the electronic voting and counting processes," Mr Green [the ACT Electoral Commissioner] said.

I hope Murphy is not eligible to vote.

[Actually, given the flakiness and lack of security in existing all-electronic voting systems, it is likely that Murphy's entire surrogate extended family will be able to vote repeatedly, many times over. PGN]

---

## **Australians voice anger over online spying**

Monty Solomon <[monty@roscom.com](mailto:monty@roscom.com)>

*Sat, 8 Sep 2001 13:08:38 -0400*

Australians voice anger over online spying

By Rachel Lebihan, ZDNet Australia News, 07 September 2001

Only three percent of surveyed ZDNet readers believe Internet Service

Providers should monitor all user activity, following a parliamentary report

that recommends user logs should be kept on customers' online activities.

The diminutive support for tighter online monitoring was transcended by a

resounding 60 percent of polled readers who said they would kick up a fuss

until the law was changed, if ISPs were forced to maintain access logs.

<http://www.zdnet.com.au/news/breakingnews/story/0,2000020826,20259325,00.htm>

---

## **World Trade Center in RISKS**

"Jay R. Ashworth" <jra@baylink.com>

*Tue, 11 Sep 2001 16:36:04 -0400*

In light of this morning's events, which I will not minimize by trying

to select an adjective to describe, I thought it might be interesting

to search the RISKS archives, and see how the building's history figures in that sphere.

First, there's coverage of the car bombing, and how the evac plan and

generators failed, in

<http://catless.ncl.ac.uk/Risks/14.37.html#subj4.1>

with follow-on in

<http://catless.ncl.ac.uk/Risks/14.38.html#subj5.1>

<http://catless.ncl.ac.uk/Risks/14.39.html#subj8.3>

There's other coverage of the bombing, as well, in <http://catless.ncl.ac.uk/Risks/14.39.html#subj8.2> which discusses how the building operators are allowed to violate the building codes that they would be otherwise bound by.

Also,

<http://catless.ncl.ac.uk/Risks/14.39.html#subj8.2>

discusses the fact that damned near every TV and most of the radio broadcast antennas serving NYC and Eastern NY State just hit the ground as well; that had to be making life miserable for people trying to get the word out.

<http://catless.ncl.ac.uk/Risks/14.41.html#subj1.1>

discusses an ATM outage in NJ attributable to the evac from that bombing.

Another outage in California happened at least in part because the backup

systems were otherwise occupied due to that same situation:

<http://catless.ncl.ac.uk/Risks/14.41.html#subj2.1>

<http://catless.ncl.ac.uk/Risks/17.17.html#subj10.1>

notes in passing that the WTC is not alone in having such problems.

[Discussion of the Citicorp problems and unlikely events. PGN]

Jay R. Ashworth, Member of the Technical Staff, Baylink, Tampa Bay, Florida

<http://baylink.pitas.com> +1 727 804 5015 jra@baylink.com

---

**✦ We only reveal a few digits of your account number, don't worry**

Dan Jacobson <jidanni@deadspam.com>

12 Sep 2001 13:04:10 +0800

> Re: Consumer Reports password policy risks (Bumgarner, [RISKS-21.65](#))  
> ... but does give the last five digits

Sounds like the Taiwan power company sending bills with only the last few digits of your auto-payment bank account revealed, the phone company sending theirs with only the first few digits revealed. Steal two envelopes and you've got the account number?

<http://www.geocities.com/jidanni/> Tel+886-4-25854780

---

## **X-ray machine risk**

Asa Bour <bourea@scripturememory.org>  
*Thu, 27 Sep 2001 23:16:04 -0400 (EDT)*

I had to get some x-rays recently. I felt real confident when I saw a bright yellow post-it note on the x-ray machine with bold print stating that the measurements were in mm (millimeters) and not in cm (centimeters). Since the note was needed, one can assume they had problems with people calibrating the machine properly with the right units. I think the x-ray software interface needs some improvement to eliminate this danger of miscalibration.

E. Asa Bour <bourea@scripturememory.org>  
<http://www.scripturememory.org/> <http://www.schemer.com/>

## **✶ Increasing RISKS of UPPER CASE**

Stuart Prescott <s.prescott@chem.usyd.edu.au>

*Mon, 24 Sep 2001 16:18:34 +1000*

I recently received a confirmation e-mail from an Australian domestic airline confirming a booking I had made over the web. The entire e-mail was in capitals (were they shouting at me or was it all "very important"?) including a little URL at the bottom for more information on in-flight health:

```
> SOME STUDIES HAVE CONCLUDED THAT PROLONGED IMMOBILITY MAY BE
> A RISK
> FACTOR IN THE FORMATION OF BLOOD CLOTS IN THE LEGS,
> (DVT - DEEP VEIN THROMBOSIS). IF YOU FEEL YOU MAY BE AT RISK
> FROM
> DVT OR OTHER HEALTH PROBLEMS, QANTAS RECOMMENDS YOU CONSULT
> WITH
> YOUR DOCTOR BEFORE TRAVEL. INFORMATION ON HEALTH ISSUES CAN BE
> FOUND ON OUR WEBSITE -
> WWW.QANTAS.COM.AU/FLIGHTS/ESSENTIALS/HEALTHINFLIGHT.HTML,
> IN OUR TIMETABLE AND INFLIGHT MAGAZINE OR CONTACT YOUR LOCAL
> QANTAS
> OFFICE.
```

No prizes for guessing whether or not the all-upercase URL works...

So the RISKS... other than making the entire message much harder to read, you can also break things.

---

## **✶ 2002 USENIX Annual Technical Conference - Call for papers**

Ann Tsai <mktgadm@usenix.org>

Tue, 18 Sep 2001 13:34:59 -0700

2002 USENIX Annual Technical Conference, June 9-14, 2002,  
Monterey, CA

<http://www.usenix.org/events/usenix02/>

Submissions to the General Refereed Sessions Track are due on  
November  
19, 2001.

FREENIX is a special track within the USENIX Annual Technical  
Conference  
that showcases the latest developments and applications in freely  
redistributed technology. The FREENIX track covers the full  
range of  
software and source code including but not limited to Apache,  
Darwin,  
FreeBSD, GNOME, GNU, KDE, Linux, NetBSD, OpenBSD, Perl, PHP,  
Python, Samba,  
Tcl/Tk and more.

The FREENIX program committee is looking for papers about  
projects with a  
solid emphasis on nurturing the open source/freely available  
software  
community and talks which advance the state of the art of freely  
redistributable software. Areas of interest include, but are not  
limited

Submissions to the Freenix Track are due on November 12, 2001.

Submission guidelines and conference details are available on  
our Web site:

<http://www.usenix.org/events/usenix02/cfp/>

The 2002 USENIX Annual Technical Conference is sponsored by  
USENIX, The Advanced Computing Systems Association. [www.usenix.org](http://www.usenix.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 21: Issue 68**

**Monday 8 October 2001**

## Contents

- [Rocket plunges into Indian Ocean](#)  
[PGN](#)
- [New interest in network security](#)  
[NewsScan](#)
- [Another unitary transformation](#)  
[Rodney Polkinghorne](#)
- [AOPA's TurboMedicalsm eases medical application process](#)  
[Richard Glover](#)
- [Ham radios in the aftermath of 11 September 2001](#)  
[Richard Murnane](#)
- [11 Sep 2001: Risks of electronic surveillance](#)  
[Gisle Hannemyr](#)
- [Re: "The Risks Are Obvious"](#)  
[Amos Shapir](#)
- [Risks of bogus e-mail addresses "FROM: ObL"](#)  
[Peter Wayner](#)
- [Remote control of airliners](#)  
[Steve Bellovin](#)
- [Re: Oxygen tank kills MRI exam subject](#)  
[Leonard X. Finegold](#)

- [MS Front Page 2002 Licence Agreement](#)  
[Alistair McDonald](#)
  - [Re: Creator of Kournikova virus gets 150 hours ...](#)  
[Gene Berkowitz](#)
  - [Re: Hacker re-writes Yahoo!](#)  
[Mark Hull-Richter](#)
  - [Trusted Computing, and Embedded and Hybrid Systems - new NSF programs](#)  
[Wm Randolph Franklin](#)
  - [Computer Security Applications Conference + Advance Program](#)  
[Jay Kahn](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

## ✶ Rocket plunges into Indian Ocean

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

Sat, 22 Sep 2001 09:01:03 -0700 (PDT)

On 21 Sep 2001, a Taurus rocket went off-course 83 seconds after launch.

Carrying an Orbital Imaging satellite, a NASA ozone-monitoring QuikTOMS

satellite, and the cremated remains of 50 people (\$5300 each), the rocket

failed to reach its intended altitude and velocity despite an attempted

correction, resulting in loss of the payloads. NASA's share of the cost was

estimated at \$50M. It was the second Orbital Sciences rocket lost in less

than four months. [Source: AP item in Newsday.com, 22 Sep 2001, PGN-ed]

---

## ✶ New interest in network security

"NewsScan" <newsscan@newsscan.com>

*Tue, 02 Oct 2001 08:39:44 -0700*

Security companies are being deluged with business opportunities, and CEO Peggy Weigle of the Internet security firm Sanctum explains, "Network security used to be a necessary evil, but now it's a core value of companies." Doing security audits commissioned by 300 organizations, Weigle found the results "scary" and said, "We could have stolen flight manifests, personnel files, sensitive data... We could have easily gotten onto a flight illegally." Research firms Gartner and IDC predict that the network security market in the U.S. will grow 20% to 24% a year between now and 2005. [USA Today 2 Oct 2001; NewsScan Daily, 2 Oct 2001] <http://www.usatoday.com/life/cyber/tech/2001/10/2/network-security.htm>

---

## **✶ Another unitary transformation**

Rodney Polkinghorne <rodneyp@raman.physics.uq.edu.au>

*Mon, 08 Oct 2001 10:14:17 +1000*

Nature, the journal that told us about cold fusion, posts summaries of recent physics papers at <<http://www.nature.com/physics/>>. One of these, "Bose, Einstein and chips," reads:

On the atom chip, the magnetic potential minimum that confines the atoms is barely a millimetre or so wide, and it holds the

condensate an ultracold cloud of around 1,600 rubidium atoms about 70-440 mm above the chip surface.

Or, as a read-source-ful scientist might discover:

about 70#150;440 <span class="symbol">m</span>m above the chip surface.

The online version of the article they are summarising [W. Hansel et al., Nature 413 p498 (2001)], gives the correct height of 70-440 micrometres.

The micro symbol is included in ISO 8859-1.

Unlike the ohm/watt confusion reported earlier (Rolph, [RISKS-21.29](#) and Peuhkuri, [RISKS-21.33](#)), millimetres and micrometres have the same dimensions. At least with SI you are always out by a factor of 1000 or more, which readers of Nature should notice. But given what you would have to pay to see that page for yourself, you would think they could afford a proof reader.

Rodney Polkinghorne

---

## **✶ AOPA's TurboMedical(sm) eases medical application process**

Richard Glover <rglover@lunarpoodle.com>

*Tue, 04 Sep 2001 09:50:24 -0700*

From: <http://www.aopa.org/whatsnew/newsitems/2001/01-3-042.html>

AOPA's TurboMedicalsm eases medical application process, 24 Aug 2001

AOPA has launched a new, Web-based tool to help pilots prepare

to obtain their medical certificates. AOPA's TurboMedicalsm is the first of a series of "intelligent" online forms to come from AOPA. Pilots who use TurboMedicalsm will be less likely to have FAA delay or deny the issuance of their medical certificate.

"AOPA's Web site ([www.aopa.org](http://www.aopa.org)) offers more resources to pilots than any other aviation site on the Internet," said AOPA President Phil Boyer.

"TurboMedicalsm is an innovative way to use the Web to remove some of the uncertainty of applying for a medical."

The innovative online form "interviews" the pilot to ensure that all of the information on FAA's Form 8500-8 (application for an airman medical certificate or student pilot certificate) is filled in correctly.

TurboMedicalsm checks the pilot's answers, and flags anything that might cause problems in issuing a medical certificate.

"FAA's Aeromedical Certification Division is currently taking up to three months to review medical applications," said Gary Crump, AOPA director of medical certification. "Some 30 percent of those delays are caused by simple errors on the application form."

TurboMedicalsm checks for those errors.

The online form takes pilots step-by-step through the 20 question areas on the medical application form. For each question, the form explains exactly what FAA is looking for and why it is asking the question. And there are links to AOPA's expansive online medical data for more

information.

The form provides advice on the best way to answer each question. For example, TurboMedicalsm tells a pilot that it is usually best to apply for the lowest class of medical that you actually need. Under FAA regulations, even CFIs need just a Third-Class medical certificate to provide flight instruction for compensation, although employers may require a higher class of medical.

TurboMedicalsm is particularly useful in helping the pilot answer the medication, medical history and medical visit questions.

When a pilot answers the question, "Do you currently use any medications?"

TurboMedicalsm checks the answer against AOPA's list of FAA-accepted drugs.

For example, TurboMedicalsm will tell a pilot that the popular over-the-counter drug Benadryl is acceptable to FAA as long as the pilot waits 24 hours after taking it before flying.

But if the drug isn't on the list, TurboMedicalsm will flag it and provide links to more information. There is even a direct email link to AOPA's medical experts so the pilot can ask specific questions.

If a pilot answers "yes" to one of the medical history questions, TurboMedicalsm will search for key words in the explanation to be able to provide more information to the pilot.

A pilot can skip a question and return to it later. TurboMedicalsm will temporarily store the answers. A pilot can choose how long TurboMedicalsm will store the answers.

Once a pilot has completed all of the questions, TurboMedicalsm will review the form for completeness and accuracy. The pilot can then print out a copy to take to the medical examiners office. Pilots should also keep a copy in their personal records.

"TurboMedicalsm is an educational, self-help tool to help pilots prepare to complete the medical form in the doctor's office," said Crump. "But for the future, we're working on an 'FAA-approved' version of TurboMedicalsm that you can complete online and email to your FAA designated medical examiner prior to the examination."

The 375,000-member Aircraft Owners and Pilots Association is the world's largest civil aviation organization. More than one-half of the nation's pilots are AOPA members.

#### RISKS Comments:

1. I am no expert, but I question the assertion "All of a pilot's answers on the TurboMedical(sm) form remain absolutely confidential. No one but the pilot will ever have access to the medical information. Data is stored on a secured server and data transmissions are encrypted." We have been told \*many times\* in other contexts that certain medical data is confidential, but absent a doctor-patient relationship, I think this is generally a very tenuous assertion. I am pretty sure there is no doctor-patient relationship created with this form.

2. "[D]ata \*transmissions\* are encrypted...." (emphasis added) is not synonymous with "the data is encrypted." If the data is stored on a secure server without encryption, it is still readable by anyone with access to the machine. If the data is encrypted where it is stored, only the person (with well-publicized exceptions) with the "keys" can access it. There is a world of difference.

3. The data is stored on a secure server, but I really don't know what that means. I think my IRS data is on a "secured server," but how many stories do we see where that data has leaked out? Medical data is \*far\* more sensitive to release than financial data, and I am less concerned with interception in transit than I am with security breaches from the server where the data is.

4. If data is stored "on a secured server" for a specific period of time, what becomes of the routine backups made? Are they periodically destroyed? If not, this information is probably obtainable indefinitely.

5. Are the links to the medications database stored? If I check on a medication, is the fact I did so recorded? It probably is on my client, and I wonder what "cookies" are employed.

6. I have not used the system (nor am I likely to), but I wonder what "disclaimers" are associated with using it. This kind of information might fall under the Fair Credit Reporting Act (which can have a very broad reach), and a user might have to authorize far more than what is

advertised.

The RISKS of this system far outweigh its usefulness. We need a machine to tell us how to fill out a form? If you have medical issues, you discuss them with your \*doctor\*, and he fills out a form. For a fee, of course, but I for one, am willing to pay a reasonable fee for privacy.

---

## ✶ Ham radios in the aftermath of 11 September 2001

Richard Murnane <RichardM@AttacheSoftware.com>

*Tue, 2 Oct 2001 11:25:10 +1000*

As others have noted, the terrorist attacks of 11th September caused major disruption to land-line and cellular phone communications. What hasn't been widely reported is that 570 Amateur (ham) Radio operators from 35 states and two Canadian provinces provided auxiliary radio communications to relief agencies operating in the affected areas.

The lesson is that even the most modern communications technology can fail, and that there is still value in having an independent communications infrastructure, especially when it costs the community little or nothing to maintain it.

Richard Murnane, Australian Amateur Radio station VK2SKY

## **11 Sep 2001: Risks of electronic surveillance**

Gisle Hannemyr <gisle@hannemyr.no>

*Thu, 04 Oct 2001 12:34:35 +0200*

In the aftermath of the September 11 terrorist attacks on the USA, a special feature on automatic electronic surveillance (i.e. Echelon, Carnivore, spy satellites, and all that) was broadcast by the BBC ClickOnline, hosted by Stephen Cole, Sep. 22).

The feature included a lengthy interview with Dr. Kevin O'Brian of RAND Europe about the failure of US intelligence to gather enough information to pre-empt the attacks. Of particular interest to RISKS readers is the following quote from Dr. O'Brian:

"We've seen reports that they may have actually been spoofing or misdirecting intelligence services quite knowingly, and that they are aware of the fact that they could use the technology against the intelligence services by sending out false signals by sending out false reports and rumours, by using technology such as mobile phone communications or Internet messages to actually misdirect the intelligence services' gaze away from their attacks."

The risks are obvious: The over-reliance on massive computer-based automatic systems for scanning and filtering that has characterised much of US intelligence gathering in the post-soviet era can only be effective as long as the bad guys are not aware of what you are doing. The simple

fact that computers systems are rule-based (and AI-systems exceedingly so) permit enemy agents to play clever counter-intelligence games, where plotting the response to certain stimuli can be used to "map out" in detail how an automatic surveillance system will respond to diverse inputs and hence "learn" how to misdirect the system on a massive scale.

A human-based intelligence system, in particularly a highly organized one, is of course also vulnerable to this type of attack, but the rule-based nature of an AI-based system makes the attack easier and more reliable

- gisle hannemyr ( gisle@hannemyr.no - <http://hjem.sol.no/gisle/> )

---

## ✶ Re: "The Risks Are Obvious"

Amos Shapir <amos@sela.co.il>  
*Thu, 20 Sep 2001 11:08:04 +0300*

I first learned of the event by connecting to a local news site here, at about 4 p.m. local time (which was 9 a.m. EDT). At first try, the site was down; when I finally got in and looked at the headline "Two Airliners crash on NY's WTC" my first reaction (probably the result of reading too many RISKS issues) was "they let their test page leak out as if it were real news"...

It seems that this "this isn't happening" initial reaction was shared by many, even some to whom this was actually happening. This had never happened before, and even though technically possible, the perceived risk of its realization was considered unreal.

The main risk is, IMHO, of evaluating the relative costs and benefits of preparing for an eventuality which, by our common sense, is very improbable; while the perpetrators seem to be making their evaluations by a completely different set of priorities and morals. How do we apply "crazy logic" to risk assessment? When do we apply it, and how crazy can we get before making the very notion of assessment senseless?

Amos Shapir, Sela Software Labs, Ltd. 14 Baruch Hirsch st.,  
Bnei Brak  
51202 ISRAEL Tel: +972 3 6176037

---

## **✶ Risks of bogus e-mail addresses "FROM: ObL"**

Peter Wayner <pcw@flyzone.com>  
*Wed, 3 Oct 2001 14:11:16 -0400*

Sincerely yours, \*Not\* Osama bin Laden?

A Filipino in Belgium ended up in jail after \*receiving\* a joke e-mail seemingly from Osama bin Laden (but apparently from one of his friends), asking to "stay with you for a couple of days." The man was freed only after a Catholic priest vouched for him as a regular attendee each Sunday.

[<http://www.vnunet.com/News/1125822>]

Ah, there's nothing like putting faith in identity, keyword scanning surveillance, and data stored in computers.

---

## ✶ Remote control of airliners

Steve Bellovin <smb@research.att.com>

*Mon, 01 Oct 2001 22:25:03 -0400*

The Associated Press reported on a test of a remotely-piloted 727. The

utility of such a scheme is clear, in the wake of the recent attacks;

to the reporter's credit, the article spent most of its space discussing whether or not this would actually be an improvement. The major focus of the doubters was on security:

But other experts suggested privately that they would be more concerned about terrorists' ability to gain control of planes from the ground than to hijack them in the air.

I'm sure RISKS readers can think of many other concerns, including the accuracy of the GPS system the tested scheme used for navigation (the vulnerabilities of GPS were discussed recently in RISKS), and the reliability of the computer programs that would manage such remote control.

---

## ✶ Re: Oxygen tank kills MRI exam subject ([RISKS-21.67](#))

"Leonard X. Finegold" <L@drexel.edu>

*Mon, 1 Oct 2001 23:29:14 -0400*

[Leonard X. Finegold, Physics, Drexel University (3141 Chestnut Street)

Philadelphia PA 19104 U.S.A. (215) 895-2740 (allow 5 rings)]

Volume 345:1000-1001, 27 Sep 2001, Number 13

Preventable Deaths and Injuries during Magnetic Resonance Imaging

To the Editor: In July, a six-year-old child undergoing magnetic resonance

imaging (MRI) in New York suffered a skull fracture and intracranial

hemorrhage after an oxygen tank that had been brought into the room was

pulled into the machine at high speed. He died two days later [1].

Undetected or misplaced metal objects have caused numerous injuries during

MRI. Twenty-four of 46 MRI facilities responding to a survey in 1999 (52

percent) reported the occurrence of MRI-related accidents [2]. Large

objects involved in such incidents included an intravenous-drug pole, a

toolbox, a sandbag containing metal filings, a vacuum cleaner, mop buckets,

a defibrillator, and a wheelchair, among others. Five incidents involving

oxygen or nitrous oxide tanks, one of which caused facial fractures, have

recently been reported [3].

To prevent such incidents, most imaging facilities currently provide safety

training to employees and administer patients a standardized questionnaire

about implants and other embedded foreign bodies before an MRI examination

is performed. Although these efforts prevent many injuries, they are

inherently limited. System-wide strategies to decrease the

incidence of serious errors are important.<sup>4</sup> Safety interventions that work continuously and automatically are generally far more effective than efforts to train large numbers of employees or to enlist the assistance of large numbers of patients.

The use of metal detectors over the doors of MRI examination rooms could have prevented every one of the large metal objects listed above from being brought into the MRI rooms and would have prevented the recent death in New York. Highly sensitive walk-through metal detectors, such as those used in airports, are available commercially for about \$2,000 to \$5,500 and require minimal maintenance. By comparison, a typical MRI unit costs approximately \$1.3 million annually to operate and generates net revenues of \$1.8 million during use in more than 3000 patients, resulting in an annual net profit of approximately \$500,000 [5]. The cost of installing a metal detector could thus easily be paid for with operating revenues. Factoring in liability savings would further decrease real costs.

Metal detectors should not replace the screening protocols currently in use, since the detectors may be insufficiently sensitive to detect small implanted metal objects, such as aneurysm clips or cardiac pacemakers. Their installation would, however, be an inexpensive, simple, and potentially life-saving addition to current practice.

Christopher Landrigan, M.D., M.P.H.  
Children's Hospital, Boston, MA 02115

landrigan\_c@hub.tch.harvard.edu

1. Chen DW. Boy, 6, dies of skull injury during M.R.I. The New York Times. July 31, 2001:B1, B5.
2. Chaljub G, vanSonnenberg E, Johnson RF Jr. Accidents and incidents in MRI: a questionnaire. AJR Am J Roentgenol 1999;172:Suppl:14-14.abstract
3. Chaljub G, Kramer LA, Johnson RF III, Johnson RF Jr, Singh H, Crow WN. Projectile cylinder accidents resulting from the presence of ferromagnetic nitrous oxide or oxygen tanks in the MR suite. AJR Am J Roentgenol 2001;177:27-30. [Abstract/Full Text]
4. Kaushal R, Bates DW, Landrigan C, et al. Medication errors and adverse drug events in pediatric in-patients. JAMA 2001;285:2114-2120. [Medline]
5. Evens RG, Evens RG Jr. Analysis of economics and use of MR imaging units in the United States in 1990. AJR Am J Roentgenol, 1991;157:603-607. [Abstract]

---

## **MS Front Page 2002 Licence Agreement**

Alistair McDonald <alistair@bacchusconsultancy.com>

*Fri, 21 Sep 2001 09:58:22 +0100*

Slashdot <http://slashdot.org/article.pl?sid=01/09/20/1443226>

reports that

the latest MS Front Page licence agreement prevents you from any anti-microsoft Web content with it:

"You may not use the Software in connection with any site that disparages

Microsoft, MSN, MSNBC, Expedia, or their products or services ..."

I always click through licences these days, so I wouldn't have read it (not that I'd install Front Page anyway), but what is the world coming to! Is this legal in your country?

Alistair McDonald                      Bacchus Consultancy                      www.  
bacchusconsultancy.com

[UCITA ([RISKS-21.27,45,41](#)) seems to make this legal in those states in

which UCITA has passed (at least Virginia and Maryland).  
Incidentally,

The Risks Forum tries to be an equal-disparager forum, but it is worth

noting for the record that each issue is prepared using Gnu-emacs on

Linux. PGN]

---

## ⚡ **Re: Creator of Kournikova virus gets 150 hours ... ([RISKS-21.67](#))**

"Gene Berkowitz" <geneb@ma.ultranet.com>

*Tue, 02 Oct 2001 00:15:41 -0400*

"... The American investigation service FBI reported an amount of \$166.827

in damages." [Translation from Dutch]

Needless to say, I don't think the FBI calculated the damages to the nearest

tenth of a cent. As is European custom, the period (.) is used as a thousands

separator, while the comma (,) is used as the decimal point. So, is one hundred and sixty-six thousand dollars (\$166,827) limited damage?

If so, Mr. De W.'s time is apparently worth over one thousand dollars per hour...

--Gene Berkowitz

---

## ⚡ Re: Hacker re-writes Yahoo! (Stock, [RISKS-21.67](#))

Mark Hull-Richter <Mark.Hull-Richter@quest.com>

*Tue, 2 Oct 2001 11:56:13 -0700*

Respected news outlets? Respected by whom? And since when does Yahoo! rate?

RISK: Assuming that there is such a thing as a "respected news outlet" and that the "news" presented has some resemblance to news (i.e., unbiased information) instead of the usual propaganda.

P.S.: Remember, the "liberal press" myth is dead and buried.

Mark Hull-Richter, Senior Programmer, Quest Software

---

## ⚡ Trusted Computing, and Embedded and Hybrid Systems - new NSF programs

"Franklin, Wm Randolph" <wfrankli@nsf.gov>

*Fri, 14 Sep 2001 16:05:21 -0400*

The Computer-Communications Research Division (C-CR) of the Computer and Information Sciences and Engineering Directorate (CISE) of the US National Science Foundation (NSF) is pleased to announce two new programs whose goal is reducing the number of submissions to this valuable newsgroup, comp.risks. For each, the due date is 5 Dec 2001, and \$4M-\$6M may be available to support 20-25 awards, subject to the usual caveats.

\*\* Trusted Computing (TC), NSF 01-160,  
<http://www.nsf.gov/cgi-bin/getpub?nsf01160>

TC seeks to establish a sound scientific foundation and technological basis for managing privacy and security in a world linked through computing and communication technology. This research is necessary to build the secure and reliable systems required for today's and tomorrow's highly interconnected, information technology enabled society. The program funds innovative research in all aspects of secure, reliable information systems, including methods for assessing the trustworthiness of systems.

\*\* Embedded and Hybrid Systems (EHS), NSF-01-161,  
<http://www.nsf.gov/pubs/2001/nsf01161/nsf01161.html>

Past research in embedded systems has focused primarily on resource-impooverished computational environments: algorithms and software that must execute on memory-, processing-, and power-constrained processors. The computational design was simple and synchronous to maximize effective operating rates, and a great deal of design effort went into optimizing performance under these conditions. As processing speed and data capacity have increased and demands for automation have expanded, the nature

of the problem has changed. Now, hard and soft real-time processes must interact, and they may be required to share the same resources. Applications such as distributed control demand communication, which introduces variability in operation. A scientific foundation currently is lacking for systematic development and integration of physical and computational components in embedded systems. This lack is particularly severe for increasingly complex, distributed embedded systems. Empirical reports show that relying on brute-force testing for verification and validation of software for modern embedded systems can push certification costs to at least half the total cost of the software. Scientific principles and supporting technology are needed to assure that requirements are met during development of software-based systems, in order to reduce the cost of evaluating dependability and certifying that a system is fit for operation. NSF investment is critical to sustain, adapt, and expand the National research and development capacity in embedded systems.

I am your humble scribe for the programs' officers, who are:

\* Dr. Helen Gill, Program Director, CISE, C-CR, 1145,  
1-703-202-8910, hgill@nsf.gov

\* Ms. Carmen Whitson, Associate Program Director, CISE, C-CR,  
1145,  
1-703-292-8910, cwhitson@nsf.gov

Please contact them for more info.

Wm Randolph Franklin, Program Director  
Numeric, Symbolic, and Geometric Computation, CISE/C-CR. Room  
1145

National Science Foundation, 4201 Wilson Blvd, Arlington VA  
22230

1-703-292-8912, fax: 703-292-9059 email: WFRANKLI@NSF.GOV

Relevant due dates:, FY02: Regular NSG: Nov 5.

Large ITR preproposals: Nov 9, Medium ITR: Nov 13, Small ITR:  
Feb 7.

---

## Computer Security Applications Conference + Advance Program

Jay Kahn <jkahn@mitre.org>

Sun, 30 Sep 2001 22:20:49 -0400

17th ACSAC, 10-14 Dec 2001, New Orleans, Louisiana, USA.

The 17th ACSAC Committee is pleased to announce the availability of the

Advance Program for the 17th Annual Computer Security Applications

Conference (ACSAC) on our web site at <http://www.acsac.org>. The Advance

Program is available in HTML for web viewing and also in PDF format for

downloading and printing. If you need a hard copy of the Advance Program,

please send your name and mailing address to

Publicity\_Chair@acsac.org, and

we'll mail you a copy.



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 21: Issue 69**

**Monday 15 October 2001**

## Contents

- [New class of wireless attacks](#)  
[Gary McGraw](#)
- [Reducing risks to hospital patients](#)  
[Mike Martin](#)
- [Ukraine missile apparently downs Russian airliner](#)  
[Hanan Cohen](#)
- [SirCam redux](#)  
[Gavin Scott](#)
- [A risk from Excel and Outlook](#)  
[Will Middelaer](#)
- [Outlook for Thanksgiving](#)  
[Patrick Lincoln](#)
- [Billion-seconds bug](#)  
[Massimo Dal Zotto](#)
- [Risks of undocumented 'standards'](#)  
[Lloyd Wood](#)
- [Re: Ham radios in the aftermath of 11 September 2001](#)  
[Todd Jonz](#)  
[Mitch Collinsworth](#)
- [Re: Remote control of airliners](#)

[Alan Wexelblat](#)

● [Re: Sincerely yours, \\*Not\\* Osama bin Laden?](#)

[Nick Brown](#)

● [Re: TurboMedical](#)

[Dick Karpinski](#)

● [Public information campaign on privacy](#)

[Ben Hutchings](#)

● [Re: Hackers and others win big in Net casino attacks](#)

[R.S. Heuman](#)

● [REVIEW: "The CERT Guide to System and Network Security Practices", J.H. Allen](#)

[Rob Slade](#)

● [Info on RISKS \(comp.risks\)](#)

---

## ⚡ New class of wireless attacks

Gary McGraw <gem@cigital.com>

*Mon, 15 Oct 2001 08:30:07 -0400*

Bob Fleck, a security consultant at Cigital, working with Jordan Dimov, has discovered new class of wireless attacks that can be used to gain unauthorized access to normally-protected machines on a standard wire-based internal network. Wireless networks involve installation of a wireless Access Point on a normal internal network. This Access Point is usually connected to the wired network through a switch or a hub. The attacks discovered by Cigital are based on an adaptation of a well understood network attack from the non-wireless world known as ARP cache poisoning. This emphasizes the importance of re-considering old risks in light of new technologies, something that is especially important in

software-based  
systems!

The new class of attacks encompasses:

- 1) the ability to monitor and manipulate traffic between two wired hosts behind a firewall
- 2) the ability to monitor and manipulate traffic between a wired host and a wireless host
- 3) the ability to compromise roaming wireless clients attached to different Access Points
- 4) the ability to monitor and manipulate traffic between two wireless clients

Previous wireless attacks have demonstrated that wireless traffic on an 802.11b network is vulnerable to monitoring and manipulation, even when it is "protected" with WEP encryption. This new class of attacks discovered by Cigital is based on abusing the Address Resolution Protocol (ARP) which binds internal IP addresses to ethernet addresses.

Mitigating the risks of these attacks is possible. The best fix involves placing a technical barrier between the wireless network and the normal wired network. This provides only a partial solution that leaves the wireless network in a compromised state, though it protects against the worst of the attack class Cigital discovered. Further risks can be mitigated through advanced design of any and all software applications that make use of the wireless network.

Bob Fleck (fleck@cigital.com) and Gary McGraw (gem@cigital.com)

For more, see:

<http://www.cigital.com/news/wireless-sec.html>

<http://www.digital.com/news/wireless/faq.html>

---

## ✶ Reducing risks to hospital patients

"Martin, Mike" <mike.martin@eds.com>

*Fri, 5 Oct 2001 15:06:50 +1000*

Spectacular accidents to hospital patients are always newsworthy.

Recent cases include a patient in the UK who died after the wrong kidney was

removed, and a boy killed by a flying oxygen cylinder ([RISKS 21.55](#)). But

according to Dr Brent James, Executive Director of Intermountain Health Care

in Utah, the overwhelming majority of cases of patient harm are from

mundane, and preventable, causes.

Interviewed recently on Australia's Radio National by Dr Norman Swan,

<http://www.abc.net.au/rn/talks/8.30/helthrpt/stories/s380415.htm>

<<http://www.abc.net.au/rn/talks/8.30/helthrpt/stories/s380415.htm>> , James

said that of 3996 cases of moderate or severe adverse drug events that his

organisation identified over a ten year period, only 3.5 per cent resulted

from a human error. The rest of the confirmed 4155 human errors over the

period "were caught before they actually led to injury, or the patient

suffered such a minor consequence that it wasn't classified as an injury".

In other words, concentrating on human error will cause 96.5 per cent of

injuries to be overlooked.

Furthermore, James said that the majority of adverse drug events were not reported through the voluntary reporting system on which most hospitals depend, and indeed many are not being even recognised by patient care staff.

Using a computer-based system to detect evidence of morphine overdoses, James found that 80 (yes, eighty) times as many events were occurring as were being reported. By using a computer system containing information about drugs' potential for allergy reactions, and that tailored drug doses specifically to each patient, his organisation has been able to cut the adverse drug event rate associated with such reactions by more than 50 per cent.

A simple systems change in treatment of patients with congestive heart failure in his organisation means, James estimates, that 310 lives are being saved each year, patients who otherwise would have died.

It seems people in the health system are beginning to apply principles long used by safety analysts in aviation and other industries. (James was a member of the Quality of Health Care in America Committee of the Institute of Medicine that created the 1999 report, "To Err is Human". Its executive summary noted, "Health care is a decade or more behind other high-risk industries in its attention to ensuring basic safety.")

The key principles in James's attack on the problem appear to be:

- \* focus on injuries, rather than human errors;
- \* encourage (and indeed reward) injury reporting (and protect from

victimisation);

- \* improve systems so that it's easy to do things right and hard to do them wrong;
- \* assign accountability for safety improvement;
- \* measure outcomes.

Use of computer technology is key to collecting and using data and instituting process control to support these principles.

On top of improving patient experience and saving lives, James said, "... the old belief that quality means spare no expense, just turned out not to be a good model. A better model is do it right the first time. It looks like that could save as much as 15% to 25% of our total cost of operations."

Mike Martin Sydney <mike\_martin@altavista.net>

---

## **✶ Ukraine missile apparently downs Russian airliner**

Hanan Cohen <hanan\_cohen@yahoo.com>

*Sat, 13 Oct 2001 06:47:31 -0700 (PDT)*

While searching for early information on the Sibir Airlines TU-154 crash,

I went to the website of Russian newspaper Pravda and was surprised to see

that they have a special section for accidents.

<http://english.pravda.ru/accidents/>

I think the editors of Pravda are RISKS readers!

Ukraine Admits Missile Might Have Downed Airliner

[[http://dailynews.yahoo.com/h/nm/20011012/wl/russia\\_crash\\_dc\\_44.](http://dailynews.yahoo.com/h/nm/20011012/wl/russia_crash_dc_44)

[html](#)]

``The cause may have been an accidental hit from an S200 rocket fired during Ukrainian exercises,' ' Evhen Marchuk, head of Ukraine's National Security Council, told a news conference to present crash investigators' preliminary findings.

The plane crash would be the second time in 18 months that Ukraine's armed forces have lost control of a live missile. Last year, four people were killed in the town of Brovary when a rocket plowed into their apartment block. The defense ministry denied responsibility for several days until rescue workers found missile parts in the rubble.

---

## ✶ SirCam redux

"Gavin Scott" <gavin@allegro.com>  
*Tue, 9 Oct 2001 14:46:34 -0700*

For the past week I've been receiving hundreds of e-mails from a user apparently infected with the "SirCam" virus.

Ho-hum, old risk, nothing new.

But in this case the virus has included an interesting document scavenged from the user's computer. The infected machine appears to belong to a Clinical Assistant Professor at the UCLA Department of Radiation Oncology, and the document is a 13 page Word .DOC form titled:

UCLA RADIATION SAFETY DIVISION  
APPLICATION for the USE of RADIOISOTOPES  
(Human Use)

and includes fields for the name, SSN, and Date-of-birth of all the personnel involved, radioactive compounds to be used, their dosages, whether the Principal Investigator has graduated from High School, and so on.

Fortunately in this case the document is not filled out, and the SirCam virus is apparently "defective" in that each time it runs it is selecting the same document to send out, but of course it's not much of a stretch to imagine even more sensitive medical documents being sprayed across the Internet indiscriminately.

Another example of an organization which Ought To Know Better failing in basic security, and of the tenacity of recent viruses (or perhaps the stubbornness of end-users) as UCLA's people have been unable to stem the tide of e-mail from the virus five days after having been informed of the problem (though their security people were quick to respond to an e-mail suggesting that medical documents were being distributed).

P.S. 22 more copies of the virus arrived during the composing of this message. Oops, 27 now.

[This risk certainly needs to be SirCamVented. PGN]

---

## **A risk from Excel and Outlook**

Will Middelaer <betamale@yahoo.com>

*Mon, 8 Oct 2001 13:05:38 -0700 (PDT)*

I stumbled across this risk when an astute coworker wondered why opening an apparently short e-mail took an inordinate amount of time to open, even for our slow connection to a remote outlook server. I sent him an e-mail composed of one short sentence of plain text followed by (what I thought was) a two column by ten row grid of excel cells. I put the cells into the e-mail by highlighting them in Excel, then copying and pasting them into an e-mail.

What I did not know was that the e-mail message actually contained the entire 12,000 plus cells of the spreadsheet including formatting and formulas. Though it appears to contain only the 20 cells that I intended to send him, double clicking the cells in the e-mail launched Excel, which opened with a complete version of the spreadsheet from which I had selected the cells to send him. The only piece of information missing seems to be the name of the file, as it opens with a generic name.

The risk: releasing quite a bit more information (plus structure of the spreadsheet itself) to an e-mail recipient to whom you intended to send only part of the spreadsheet, and the risk of an application being a bit too helpful.

(Versions are Outlook 2000 Corporate or Workgroup, Excel 2000.)

Will Middelaer <will.remove@middelaer.remove.com>

---

## ✶ Outlook for Thanksgiving

Patrick Lincoln <lincoln@csl.sri.com>

*Wed, 10 Oct 2001 07:34:46 -0700*

It seems that in some versions of Microsoft Outlook, Thanksgiving 2001 is marked as 29 Nov. In fact, Thanksgiving is early this year, on 22 Nov.

---

## ✶ Billion-seconds bug

Massimo Dal Zotto <dz@cs.unitn.it>

*Thu, 11 Oct 2001 19:56:58 +0200 (MEST)*

As everybody knows, on Sep 09 01:46:40 2001 GMT the system clock of every UNIX system made the transition from 999999999 seconds to 1000000000. After having survived the millennium bug we believed that the "billion seconds bug" wouldn't happen, since the UNIX time is stored as a 32-bit integer.

I have, however, been witness of a real "billion seconds bug" that hit a medical application distributed by a top company in the medical sector. (No, I won't name the company.)

On September 11, a colleague told me that he and other

technicians were having strange problems with an archiving application that was unable to initialize new cdroms. After a quick investigation, we discovered that the automatically generated cd label contained a UNIX timestamp that after Sep 09 01:46:40 passed from 9 to 10 characters, resulting in an invalid label not recognized by the application that was expecting a fixed-length label.

An interesting side effect of this has been a sudden rise in orders of cd-rw drives that were initially blamed as the cause of the problem.

Massimo Dal Zotto, Via Marconi, 141, 38057 Pergine Valsugana (TN) Italy  
++39-0461534251 www: <http://www.cs.unitn.it/~dz/> dz@cs.unitn.it

---

## **⚡ Risks of undocumented 'standards'**

Lloyd Wood <eep1lw@eim.surrey.ac.uk>  
*Tue, 9 Oct 2001 17:17:23 +0100 (BST)*

Andrew Tridgell is quoted as saying of the SMB protocol [[http://www.linux-mag.com/2001-07/tridgell\\_03.html](http://www.linux-mag.com/2001-07/tridgell_03.html)]:

The protocol is so incredibly convoluted and bloated and badly designed --

there are ten ways of doing everything. You end up with these massive

exchanges going on the wire between Windows 95 and NT, just because they

are trying to work out exactly which sets of bugs the other guy has so

they can figure out how to actually stat a file or find its

size or date

or something. And we've found from talking to people who work at Microsoft

how much of a headache it is to maintain the damned thing and keep it

secure. So, they've got to be thinking of dropping it at some stage.

As also shown by Microsoft's office document formats (RISKS passim), the

risk here is that an unpublished design with gradual increments and a focus

on implementation interoperability at all costs leads to baroque, complex

implementations, a shifting feature set, and emergent, undesirable side

effects. It's like building on sand; eventually you spend all your time just

shoring up the existing structure.

There's a lot to be said for having published, fixed revisions of documented

standards, for implementations to adhere to, in minimising such risky

interactions.

<L.Wood@surrey.ac.uk>PGP<<http://www.ee.surrey.ac.uk/Personal/L.Wood/>>

---

## **✉ Re: Ham radios in the aftermath of 11 September 2001 (Murnane, [R-21.68](#))**

Todd Jonz <todd@tj.org>

*Fri, 12 Oct 2001 22:28:33 -0700*

In [RISKS 21.68](#) Richard Murnane <RichardM@AttacheSoftware.com> writes:

> 570 Amateur (ham) Radio operators from 35 states and  
two  
> Canadian provinces provided auxiliary radio  
communications...

What Richard's message didn't mention are the numerous pressures, particularly in the U.S., that put volunteer communications services like these at risk.

In the U.S. the radio spectrum used for these communications is either dedicated to the Amateur Radio Service, or shared with other services. But a variety of commercial interests, from cellular telephone companies to package shippers to low earth orbit satellites operators, have had their eye on this spectrum for quite some time and never miss an opportunity to attempt a "land grab." Unfortunately, sometimes they are successful. In this age of spectrum auctions that generate revenue for the federal government, the amateur radio community must continually struggle to retain its spectrum allocations.

Identical bills in the House of Representatives (HR 817) and the Senate (S 549) known as The Amateur Radio Spectrum Protection Act of 2001 would protect these allocations. These bills have a broad base of bipartisan support, with 44 co-sponsors in the House and seven in the Senate. Nevertheless, although these bills have been introduced in previous sessions of Congress, they have never made it to a floor vote in either house.

Additional information about The Amateur Radio Spectrum Protection Act of

2001 can be found at:

<http://www.arrl.org/govrelations/arspa-backgrounder.html>

RISKS readers who feel inclined to contact their Congressional representatives in support of these bills will have my gratitude and, I'm sure, the gratitude of the entire amateur radio community.

Todd Jonz, KB6JXT <todd@tj.org>

When cryptography is outlawed, bayl bhgynjf jvyy unir cevinpl.

---

## **⚡ Re: Ham radios in the aftermath of 11 September 2001 (Murnane, [R-21.68](#))**

Mitch Collinsworth <mitch@ccmr.cornell.edu>

*Sat, 13 Oct 2001 14:33:55 -0400 (EDT)*

And the RISK that this points out is that if local government regulations, restrictive covenants, and tenant organization rules continue to make it more and more difficult/impossible for Amateur Radio operators to put up antennas for their stations, the day will eventually come when this nearly free backup communication system will no longer be available in times of emergencies.

Hams have "been there" for their communities, nations, neighbor communities, and neighbor nations in times of trouble for many, many years. The value of their service needs to be recognized, and their right to assemble functional radio stations needs to be guaranteed rather than restricted.

Mitch Collinsworth, K2VD

---

**✈ Re: Remote control of airliners (Bellovin, [RISKS-21.68](#))**

Graystreak <wex@media.mit.edu>

*Tue, 9 Oct 2001 13:09:51 -0400*

NPR had a fairly extensive discussion of the alternate-control proposal.

One key element of the scheme being proposed is a weighted voting system, with weights assigned based on degree of deviation from preapproved flight plan.

I regret not writing down the name of the expert interviewed (though writing while driving has its own risks :). He seemed quite reasonable and spent a good portion of the interview discussing possible failure scenarios.

He noted that ground facilities such as control towers and transmission facilities are in fixed locations that are easier to secure, easier to harden, and easier to retake in the event of hostile takeover than an airplane cockpit.

If all else fails, the control signal could be sent from an alternate ground site, and this is where the discussion of the deviation-from-flight-plan algorithm came in. In essence, if the plane's control computers received conflicting signals (say, from cockpit controls and from a ground station)

they would give more weight to those signals closer to the original flight plan.

The criminal acts of 11 Sep required significant deviation from flight plans over an extended period of time. If an order to take such a significant deviation can be overridden by another order saying "stick to plan; fly to LAX; land normally there" then you reduce the number of possible disaster scenarios significantly.

Of course, this is not a total solution - we can all easily think of sequences of events that would lead to this kind of system failing. In addition, the system would need good specification in order not to interfere in standard emergency situations (onboard fire, engine failure, passenger with heart attack, etc). But a system of this sort raises the bar to hijacking substantially, requiring the acquisition and use of much higher levels of technology than simple 'box cutters.' Such technology and training is clearly not out of the reach of all criminals, but it is out of the reach of most.

I am in favor of continuing investigation and testing of such systems, as they seem more directly focused on preventing known bad scenarios. By contrast, most of the responses proposed so far by the FAA and Congress seem to have little bearing on the scenarios as we understand them at this point.

Alan Wexelblat <[wex@media.mit.edu](mailto:wex@media.mit.edu)> <http://wex.www.media.mit.edu/people/wex/>

---

**✶ Re: Sincerely yours, \*Not\* Osama bin Laden? ([RISKS 21.68](#))**

Nick Brown <Nick.BROWN@coe.int>

*Thu, 11 Oct 2001 14:24:04 +0200*

>A Filipino in Belgium ended up in jail after \*receiving\* a joke e-mail

It turns out on reading the article that the message in question was an SMS

text message sent on a GSM phone. I cannot believe that the people who (in

the name of freedom of course) monitor telephone traffic are grepping SMS

messages for "Osama bin Laden", on the off chance that he signs them

himself. But if they are doing so, I guess they're reading this too, so "hi guys" !

Nick Brown, Strasbourg, France

---

**✶ Re: TurboMedical ([RISKS-21.68](#))**

Dick Karpinski <dick@cfcl.com>

*Tue, 9 Oct 2001 00:56:09 -0700 (PDT)*

The RISK I noticed in TurboMedical (sm) is that it instructs the applicant

in exactly what lies to tell the FAA to get through. Thus it may be a RISK

of FAA practices rather than of the use of computers.

Dick

---

## **⚡ Public information campaign on privacy**

Ben Hutchings <ben@decadentplace.org.uk>

*Fri, 5 Oct 2001 20:04:45 +0100*

The UK's Information Commissioner, a part of the government with which databases of personal information are supposed to be registered, is running a series of poster ads encouraging people to be careful with their personal information. For example, one ad says "When your bank rings you up asking questions, do you ever make sure it really is the bank?"

While the message may be familiar to RISKS readers, it's heartening to see it brought to public attention - and somewhat surprising to those of us who consider the current government to have little regard for personal privacy.

Ben Hutchings <ben@decadentplace.org.uk> <http://womble.decadentplace.org.uk>

---

## **⚡ Re: Hackers and others win big in Net casino attacks ([RISKS-21.67](#))**

<rsh@idirect.com>

*Tue, 02 Oct 2001 10:32:58 -0400*

Your added statement to Ken Nitz' item about illegal Internet gambling parlours ignores the simple fact that they are NOT illegal in many jurisdictions outside the US, and that US law does not apply outside the US. [Also, it was two of their sites that had been hacked, not one...]

An example of the latter statement is:

<http://news.excite.com/news/ap/010919/20/australia-internet-defamation>

which is an interesting risk of publishing on the Internet where US law is NOT accepted as primary.

R.S. (Bob) Heuman, Toronto, ON, Canada

---

## **⚡ REVIEW: "The CERT Guide to System and Network Security Practices", Julia H. Allen**

Rob Slade <rslade@sprint.ca>  
*Wed, 10 Oct 2001 07:54:02 -0800*

BKCGSNSP.RVW 20010728

"The CERT Guide to System and Network Security Practices", Julia H.

Allen, 2001, 0-201-73723-X, U\$39.99/C\$59.95

%A Julia H. Allen

%C P.O. Box 520, 26 Prince Andrew Place, Don Mills, Ontario  
M3C 2T8

%D 2001

%G 0-201-73723-X

%I Addison-Wesley Publishing Co.

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

%P 447 p.

%T "The CERT Guide to System and Network Security Practices"

The preface states that the intended audience for this work is the mid-level system and network administrator. Actually, it uses the plural, giving the first indication that this text is only intended for those working in very large organizations. Chapter one is an overview of the structure of the book, along with a listing of some other resources, and a few general security definitions.

Part one deals with securing or hardening computers against attack. Chapter two lists good practices for servers and workstations, providing basic guidelines. There is something of a detailed breakdown of these conventions, as well as considerations that might be useful in policy discussions. However, these are not procedures, and there is very little in the way of system detail. The reader is advised to limit services running on computers. This is a good practice, but there is nothing to indicate how to find out what services are running, nor how to limit or eliminate them once they are found. A number of assumptions have been implicitly made, for example about centralized administration policy, so even the material that is included may not be suitable for all environments. The explanations are reasonable, but rather pedestrian, and there is a great deal of duplication of material (the sections dealing with limiting services running on servers and workstations, for example, are almost identical.) Much the same is true of securing public web servers, in chapter three. Some material

is quite specific (specifying the Common Log Format, CLF, for activity files) while other recommendations are vague. Deploying firewalls, in chapter four, is a bit different, in that it does contain some explanation of firewall types and architectures. Unfortunately, this text is very brief, and is padded out with unilluminating illustrations.

Part two examines intrusion detection practices. Chapter five covers the preparation and setup of intrusion detection, chapter six the actual detection of intrusions, and chapter seven outlines responses to intrusions. Overall, part two is more useful than part one, since intrusion detection is a newer field, and general concepts are still helpful even if specific details are lacking.

Given the complaints I have made about the lack of details, some will respond that I have, heretofore, ignored the fact that there are two appendices in the book, dealing with security implementations and practices. True, these documents exist. In terms of the security implementations, if you are using Solaris 2.x, Tripwire, Logsurfer, and Snort, the additional material may be very useful. Otherwise, it still doesn't address the lack of specifics in the book.

This work does provide the security specialist, faced with responsibility for policy creation or maintenance, a handy set of checklists and some framework for the policy process. Use of the text will help remind the

professional of areas to be addressed, and prevent certain aspects from slipping between the cracks. The advanced and experienced system administrator may also benefit from the volume, since he or she will likely already know system specifics for a number of the functions required, and probably has some idea of where to find information about others. However, intermediate sysadmins, with an "engineer" level certificate and a few years' work experience, are unlikely to know the details of security operations that have, usually, been seen as a specialty area. Therefore, the audience which will find this book to be useful is a rather narrow one.

copyright Robert M. Slade, 2001    BKCGSNP.RVW    20010728  
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 21: Issue 70**

**Friday 19 October 2001**

## Contents

- ["Glitch" assigns votes to wrong candidate](#)  
[Tom Malaher](#)
- [Pregnant chad revisited](#)  
[Douglas W. Jones](#)
- [Internet voting, revisited](#)  
[Marcus de Geus](#)
- [LA County voting machine status report](#)  
[David Schneider](#)
- [Stray bomb caused by typo](#)  
[Tim Hollebeek](#)
- [Jet engine starter motors](#)  
[Ben Laurie](#)
- [Your stolen Passport](#)  
[Monty Solomon](#)
- [Re: A Risk from Excel and Outlook](#)  
[Martin Torzewski](#)
- [Euro changeover](#)  
[Douglas Long](#)
- [Re: Outlook for Thanksgiving](#)  
[Edward Reid](#)

[Conor O'Neill](#)

● [Re: Risks of bogus e-mail addresses "FROM: ObL"](#)

[Sascha Mattke](#)

● [Improper address-change validation](#)

[Leonard Erickson](#)

● [Re: Ham radios in the aftermath of 11 Sep 2001](#)

[Jack Decker](#)

● [ACM Forum on Legal Regulation of Technology](#)

[Edward W. Felten](#)

● [International Conference on COTS-Based Software Systems](#)

[Carol Biesecker](#)

● [REVIEW: "Viruses Revealed", Robert M. Slade/David Harley/Urs Gattiker](#)

[Rob Slade](#)

● [Info on RISKS \(comp.risks\)](#)

---

## ✶ "Glitch" assigns votes to wrong candidate

Tom Malaher <risks@netstart.com>

Wed, 17 Oct 2001 23:02:27 -0600

[With Election Day coming up again (!!!) in the U.S., the first four items in this issue seem particularly relevant. PGN]

Computer glitch miscounts votes ... Just after midnight, one of them

[supporters] decided to take a last look at the results on the city's

election Web site and discovered Desbarats had won -- a computer glitch had

assigned the wrong totals to each candidate. ... The problem, said election

officials, stemmed from the fact candidate Athena d'Arras's surname starts

with a lower case "d," and the computer database that sorted election

results didn't recognize it as the first letter of her last name. "Capital

letters were sorted first and smaller letters were sorted next,  
so  
everything went in for the wrong candidate," said Barbara  
Clifford, the  
city's returning officer. [Source: \*Calgary Herald\*, 17 Oct  
2001:]

<http://www.canada.com/calgary/calgaryherald/story.asp?id={4567F15E-6CB8-4D0D-8245-31EDB555AA00}>

[My question is, why would the sort order of the output affect  
the correct  
assignment of votes to candidates? Hopefully the unique key  
being used is  
not the index position in a sorted array, but something more  
sophisticated.  
Tom M]

[Perhaps the programmer implicitly assumed the order of  
appearance was  
indeed ASCII-collating-sequence sorted! Close but no  
ASCIIgar. PGN]

---

## ✶ Pregnant chad revisited

"Douglas W. Jones" <jones@cs.uiowa.edu>  
*Fri, 19 Oct 2001 15:16:10 -0500 (CDT)*

I've recently gotten my hands on a Votomatic voting machine  
(thanks  
to Larry Mandel of Governmental Business systems Inc for sending  
it  
to me, out of the blue), and I've used it to do some experiments  
on  
pregnant chad, following up on questions arising from an  
interview  
I did with the Fort Lauderdale Sun Sentinel last December. The  
results  
of my experiments are on the web, in:

<http://www.cs.uiowa.edu/~jones/cards/chad.html>

complete with lots of pictures. In sum, certain ballot positions on a Votomatic voting machine, and not others, are particularly prone to jams caused by an accumulation of chad inside the mechanism. This was not difficult to uncover -- although punching all that chad was a bit boring.

If the election community was supported by a decent research capability, this problem with the machine ought to have been known years ago. I'm shocked that nothing was mentioned of this possibility in any of the testimony I'm aware of from last winter's legal battles or the Congressional hearings last spring, because once you take the machine apart and look at how it works, the risk is pretty obvious.

Doug Jones <jones@cs.uiowa.edu>

---

## **Internet voting, revisited**

"Marcus de Geus" <marcus@degeus.com>  
*Wed, 17 Oct 2001 02:02:48 +0000*

A Dutch RNW news mailing reports that Internet (presumably WWW) voting to find a new name for the merged towns of Leidschendam and Voorburg in the Netherlands was abandoned after large-scale fraud was suspected.

Starting on 12 Oct 2001, residents of the two towns, which are due to merge

on 1 Jan 2002, were given the opportunity to indicate their choice of names (which I won't bother you with) for the new municipality via the Internet.

On 15 Oct, 10,000 votes were counted, which was considered "an improbably high count". Also, the town councils received e-mail warnings pointing out the susceptibility to fraud of Internet voting.

As a result, the referendum will be restaged, this time using a new medium:

e-mail. Voters will be asked to leave their name and address.

I don't think there's any need to point out the RISKS.

Marcus de Geus <marcus@degeus.com> <http://www.degeus.com>

---

## **LA County voting machine status report**

"Schneider, David" <David.Schneider@Emulex.Com>

*Tue, 16 Oct 2001 18:03:48 -0700*

On the KLCS broadcast of 2001.10.10, the Los Angeles County Board of Supervisors meeting included an agenda item on digital voting machines.

I caught it in progress, but was able to make the following notes:

Conny B. McCormack, The LA County Registrar/Recorder was giving a progress report, and made the following points

- The Cal Tech/MIT report was that digital voting machines [in general?] were "not ready" for full deployment.
- Logistics: current models are heavy, increasing

transportation issues,

including delivery charges.

- Training: The decertification of [prescored] punch cards was due to 1-3%

problems that voters experienced - it can expected to be difficult to keep

new system problems that low.

- Training: LA County has to train 2500 poll workers who cover 5000 [500?]

polling places.

- Punch cards allow parking-lot setup if polling place is locked; what would

be the fallback with digital voting machines?

- Phased introduction is desirable: early voters in 2000 (9 locations 1%

of voters) and 2002, and full deploy in off-year election such as 2005.

- Paper ballots are a contingency plan; they remain certified and are

cheaper but the slow count that results is an issue.

Supervisor Knabe had the comment that he had observed, in the early voter

trial, that seniors had fear of the new machines going in, but liked the big

print; and the disabled liked voice features

Supervisor Yaroslavsky was asking what is consequences of missing the goal

of full deployment for the 2004 election, and how would the conversion be

funded? (This would be a BIG budget hit).

Ms. McCormack pointed out in other comments that LA County (among others in

California) had to respond to the California Secretary of State, but that

this was being driven by a class-action lawsuit, and the court could mandate

a stricter schedule than the Secretary of State might. Also, there was a

reference made that, "Cal Tech voting machines did not yet exist".

I hope my summary is reasonably accurate, and that the parts I missed don't change the thrust of the discussion. Meanwhile, voting officials will be watching the counties in Florida where digital voting machines would get their next big trial.

David Schneider

---

## **✈ Stray bomb caused by typo**

Tim Hollebeek <tim@hollebeek.com>  
*Mon, 15 Oct 2001 13:12:29 -0400*

Several sources are now reporting that a satellite bomb that went astray and hit a residential area did so because the pilot entered one digit wrong when entering the target coordinates.

Without more information, it is hard to say definitively how this problem could be avoided, but it certainly seems feasible that systems which display or accept GPS coordinates could use a check digit that detects one digit errors and transpositions, much like the one used in credit-card numbers.

If at all possible, systems attached to 2000-lb warheads should be as resistant to typos as commercial systems are.

Tim Hollebeek

## **✶ Jet engine starter motors**

Ben Laurie <ben@algroup.co.uk>  
*Mon, 15 Oct 2001 14:42:49 +0100*

Recently I flew from Heathrow to Boston with British Airways on (I think) a 747. My plane was delayed for two hours while one of the starter motors was replaced. We then flew to Boston without event. Whilst in Boston I joked with friends that it was kind of scary that the starter motor was replaced and tested precisely once before we flew across the Atlantic. Of course, the response (which I naturally expected) was that it only needed to work once. But is that true?

As it happened, on my return flight I spent the takeoff in the cockpit of the 777 I flew back on. As we took off, I noted that the copilot switched the starter motors to "continuous" after takeoff. When I asked why, he said that because there were a lot of clouds, the moisture could put the engines out -- so they ran them in continuous start "just in case".

So, how safe was it to fly across the Atlantic on a single test?

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

---

## **✶ Your stolen Passport**

Monty Solomon <monty@roscom.com>  
*Wed, 3 Oct 2001 22:45:59 -0400*

ZDNET, OPINION, By Wayne Rash, 26 Sep 2001

The way Dave Thomas describes it, he and his staff were trying to track down a series of unusual bugs in Windows, when they stumbled across something that really worried them. There, on their screens along with the code they were debugging, was the name and password they'd just used for Microsoft's Passport service. Worse, it was in plain text, and readily accessible. As he looked more deeply, he realized that creating a worm that could recover that information would be, in his words, "trivial."

<http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2814881,00.html>

---

## ✦ **Re: A Risk from Excel and Outlook (Re: [RISKS-21.69](#))**

Martin Torzewski <torzewsm@lch.co.uk>

*Tue, 16 Oct 2001 13:32:21 +0100*

I encountered this some years ago. See MS KB extract below (my italics).

The article goes on to provide around 3 ways of avoiding it (none being default - the risk). When I reported it the mail administrator where I worked at the time, we jointly concluded that the existence of the KB entry meant MS would be unresponsive to any report.

As it happened, what was sent to me was sensitive in terms of cell content which I shouldn't have seen.

Martin Torzewski Work: +44 (0)20 7426 7280

OL98: Entire Excel Worksheet Copied Rather than Selected Cells

The information in this article applies to:

\* Microsoft Outlook 98

#### SYMPTOMS

Double-clicking a selection of cells that are pasted from Microsoft Excel into a Microsoft Outlook 98 e-mail message, displays the entire worksheet rather than just the selection of cells.

#### CAUSE

This is by design. When you use Microsoft Outlook Rich Text for the default e-mail message format and you paste the cells with the Microsoft Excel worksheet still open, the default paste option is Microsoft Excel Worksheet.

<http://support.microsoft.com/support/kb/articles/Q192/4/17.ASP>

---

## Euro changeover

Douglas Long <long@lightlink.com>

*Sun, 14 Oct 2001 21:50:48 +0200*

I am trying to balance my first statement from my French bank. (For those of you not familiar with the Euro conversion, banks in France currently allow transactions in both Francs and Euros, which results in a statement that contains amounts in both currencies.) My bank provides two statements, the first in Francs and the second in Euros. Unfortunately, I

am trying to use Quicken to reconcile my account (which has its own peculiarities with respect to non-dollar currencies) and am running up against a problem with round off errors.

Converting all values to Euros and then calculating the account balance, as I do in Quicken, yields one answer. Calculating a partial balance in Francs, converting to Euros, and then completing the remaining calculations using Euros, as my bank does, yields a slightly different result. Not enough to make a difference to me, but multiplied by 1000's of bank accounts one has to wonder if anyone is taking advantage of the rounding errors?

[This possibility was suggested quite some time ago in <http://catless.ncl.ac.uk/Risks/19.69.html#subj6.1> .]

What makes me really wonder here is the way my ATM withdrawals are recorded on my statement. Every withdrawal results in Francs coming out of the machine, but some ATM transactions are reported in Francs on the Franc part of my statement and others are reported in Euros on the Euro part of my statement. This even occurs when I use the same ATM machine; some are recorded Francs, some are reported in Euros! I can think of no rational reason why this is so.

Douglas Long, Paris, France

---

**✶ Re: Outlook for Thanksgiving ([RISKS-21.69](#))**

Edward Reid <edward@paleo.org>

*Tue, 16 Oct 2001 9:48:00 -0400*

> It seems that in some versions of Microsoft Outlook,  
Thanksgiving 2001 is  
> marked as 29 Nov. In fact, Thanksgiving is early this year,  
on 22 Nov.

That's not early. Thanksgiving has always been celebrated on the  
fourth  
Thursday in November, never the fifth. (Where "always" ::= as  
long as I've  
been alive, 52 years.) The risk is not that the celebration date  
might  
change -- it didn't -- but that the programming was done by  
someone who  
didn't know the basics of the application area (holidays).

Edward Reid

---

## **⚡ Re: Outlook for Thanksgiving**

"Conor O'Neill" <ONeillCJ@logica.com>

*Tue, 16 Oct 2001 13:46:25 +0100*

Surely the real risk here is any program pretending to 'know'  
anything  
about these public holidays. For the vast majority of the world,  
the  
US-style 'Thanksgiving' holiday doesn't exist at all.

Conor O'Neill, Bristol, UK

---

## **⚡ Re: Risks of bogus e-mail addresses "FROM: ObL" (Wayner,**

## [RISKS-21.68](#)

Sascha Mattke <[mattke.sascha@guj-koeln.de](mailto:mattke.sascha@guj-koeln.de)>

*Thu, 18 Oct 2001 08:26:25 -0400*

That news is nonsense. I talked with the priest who was cited on vnunet. He said that some Filipino members of his church received that sms and were also questioned by the police (very politely, he stressed), but this was in no way related to receiving the sms. The padre basically said that the story was made up by a leftist ngo called Migrante International, then printed without research by the inquirer, and then found its way on the net. He and some Filipinos are now demanding the ngo to apologize for spreading fear with the relatives of the questioned people.

Sascha Mattke, Redaktion BIZZ, Stolberger Strasse 200, 50933 Koeln

Tel +49 (0) 221 - 5341-575 [mattke.sascha@bizz.de](mailto:mattke.sascha@bizz.de) <http://www.bizz.de>

---

### **✶ Improper address-change validation**

Leonard Erickson <[shadow@krypton.rain.com](mailto:shadow@krypton.rain.com)>

*Tue, 9 Oct 2001 04:35:52 PST*

About a month ago I decided to update some info in a personal ad on alt.com.

Among other things, I changed the e-mail address that responses were and notifications of potential matches were to to be sent to.

Imagine my surprise when I found that the confirmation message was sent  
\*only\* to the new address.

Sure, it requires a password to get logged in to alt.com. But once there,  
\*anyone\* could change the info, and the first I'd have known was when I  
couldn't get in.

While this isn't an application that can cause damage, it is one where  
the results could be more than a bit embarrassing.

The method of "verification" chosen might guard against mistyping the  
address you wished to change to, but it provides no security.

I've gotten no response to my e-mail to alt.com pointing out the flaws in  
their "security".

Leonard Erickson (aka shadow{G}) shadow@krypton.rain.com  
last resort: leonard@qiclab.scn.rain.com

---

## **✶ Re: Ham radios in the aftermath of 11 Sep 2001 (Murnane, R-21.68)**

Jack Decker <jack@novagate.com>  
*Mon, 15 Oct 2001 17:06:04 -0400*

With all due respect to Mr. Jonz and Mr. Collinsworth, the problems that  
amateur radio operators are having with government officials are, in my  
opinion, largely a product of their own attitudes. Those who promote Linux

and other alternative operating systems could take a lesson from this as well.

Not too many years ago, there was a requirement that was considered absolutely essential for getting into ham radio: That you know Morse code at 5 words per minute. That may not seem like a huge obstacle (particularly to those who found it easy) but in a way it's like playing the piano - some people pick it up naturally and can "play it by ear", some struggle with it but do well enough to get by (IF they have sufficient motivation), and some are completely tone deaf - no matter how they try, it just doesn't make sense to them. The amateur radio community has steadfastly refused to acknowledge that the latter group could even possibly exist.

But what was worse was the attitude of many hams whenever someone advocated dropping the code requirement. Their attitude was that the code acted as a "lid filter" which kept the "undesirables" (read: former CB radio operators) out of ham radio.

The result of this was that there were many kids like myself, who had the interest and knowledge of electronics back in the 60's and 70's, but who found the code an insurmountable barrier. Having been this excluded from the exclusive group of those who could "pound brass", we found it hard to figure out why we should care what happens to ham radio in the future. We moved on to other things, like computers and the Internet.

Then a little over a decade ago, U.P.S. (the folks who deliver

packages

using brown trucks) petitioned for some 2-meter frequencies that were carved right out of the ham bands. A lot of hams were so arrogant that they thought there wasn't a chance that the FCC would give away any of their precious spectrum to a commercial interest. Well, they got a rude awakening, and suddenly decided that perhaps it would be in their best interest to allow folks into certain classes of amateur radio without the code requirement, although even that did not happen without a lot of "kicking and screaming" by the older hams.

But even then, they reserved the higher classes of amateur licenses - the ones that had access to frequencies capable of spanning long distances - for those that could decipher Morse Code at a higher rate of speed. Even though some hams (and potential hams) had absolutely zero desire to communicate using Morse Code, the requirement was still forced upon them by the "old guard". Wouldn't want any former C.B.'ers communicating with people overseas, you know!

Well, guess what - that generation that the hams snubbed is the generation that's now holding political offices. Many of those who know enough about amateur radio that they are not voting out of total ignorance, also know that they were welcomed on CB and told to go study the Morse Code (already a dying form of communication) by the hams.

I see the same type of struggle happening today in the Linux community,

between those who feel that Linux should be made as easy to use as Windows, and those who feel that people ought not to even be allowed to own a computer unless they know how to use the command line interface (I've even seen a few Linux folks suggest that computer users should be licensed!). Fortunately, since the use of Linux is not licensed by any government, vendors can make their own decisions as to how much user-friendliness to incorporate into the product.

The risk is that if you set up something, be it a hobby or a computer operating system, in such a way that it appears that you are making it *\*deliberately\** harder to learn than it needs to be, some folks either cannot or will not make the effort, and those are lost opportunities for making friends. And it's also something that could come back to bite you in the butt, should those of the "excluded" class ever reach positions of power.

Personally, I have good friends who are ham radio operators and yet I still find it difficult to have much sympathy for the plight of hams as expressed by Mr. Jonz and Mr. Collinsworth. From where I sit, the hams (or at least their predecessors in the hobby) brought much of it on themselves.

Jack Decker

---

## **ACM Forum on Legal Regulation of Technology**

"Edward W. Felten" <felten@cs.princeton.edu>

*Wed, 17 Oct 2001 06:55:24 -0700*

ACM Forum on Legal Regulation of Technology  
(<http://www.cs.princeton.edu/lawtech>)

Laws and legal regulations are increasingly affecting what technologists can do. The ACM Forum on Legal Regulation of Technology is a new venue for technologists to discuss how the law is changing their work.

There are many examples of the law's impact on technology. The growth of intellectual property claims, including software and business-model patents, has affected many technologists. Prohibitions on specific technologies, such as those in the U.S. Digital Millennium Copyright Act, have affected both researchers and practitioners. Applications of antitrust law have shaped the landscape for companies both large and small.

Legal scholars have been discussing these issues for some time, but computer scientists have not been nearly as active in the debate. The forum seeks to bring technologists into the debate. Although we welcome the contributions of legal scholars, the forum belongs to technologists and has a technology-centric view.

Many discussions will necessarily focus on the laws of a particular country, often the United States, but the forum is international in scope. Discussion of any country's laws will be welcome. In light of economic globalization, international treaties, and countries' efforts to harmonize their laws with each other, we expect technologists throughout the world to face many of the same issues.

The forum will follow the model of ACM's successful RISKS Forum, issuing a periodic digest of contributions. Contributions will be chosen by a moderator, and generally will be short but may point to lengthier discussions elsewhere.

The forum is sponsored by ACM. It is hosted by the Department of Computer Science at Princeton University. The moderator is Edward W. Felten.

#### How To Subscribe:

To subscribe, send an e-mail message to majordomo@cs.princeton.edu. The body of the message should contain the single line "subscribe lawtech". If all goes well, you will receive a reply message saying that you have been subscribed to the forum.

---

## **✶ International Conference on COTS-Based Software Systems (ICCBSS)**

Carol Biesecker <cb@sei.cmu.edu>  
*Mon, 15 Oct 2001 17:31:06 +0000 (UTC)*

International Conference on COTS-Based Software Systems (ICCBSS)  
4 - 6 February 2002  
Orlando, Florida, USA  
World Wide Web: <http://www.iccbss.org>

Implementing COTS-based software systems presents unique problems that typical reuse practices do not address. As systems increasingly depend on

the successful integration of COTS products, practitioners and researchers must be ready to meet these challenges.

National Research Council Canada, the Software Engineering Institute, and the USC Center for Software Engineering present the inaugural International Conference on COTS-Based Software Systems (ICCBSS). ICCBSS is the first conference dedicated to solving the unique problems of using COTS products in large systems [\*]. We have assembled a unique program that includes keynote addresses by Barry Boehm of the USC Center for Software Engineering, David Baum of Motorola Labs, Ivar Jacobson of Rational Software, and Mike Moore of NASA. The conference features over 25 presentations covering COTS management and engineering processes, technical strategies, and practical experiences using COTS products in large systems. In addition, panel discussions will address the critical issues involved in constructing survivable systems using COTS products, testing systems incorporating COTS products, and dealing with COTS vendors.

Additional information about the program and conference registration can be found on this Web site: <http://www.iccbss.org>

Contact: Barb Hoerr, E-mail: [iccbss2002@sei.cmu.edu](mailto:iccbss2002@sei.cmu.edu), Phone: + 1 412 268 3007

[\* NOT TRUE. I keynoted a NATO conference on that subject in Brussels, April 2000. On my Web site you will find lecture notes for the talk, and references to many of the published papers given in my report on

survivable systems and networks. <http://www.csl.sri.com/neumann> PGN]

---

## REVIEW: "Viruses Revealed", Robert M. Slade/David Harley/Urs Gattiker

Rob Slade <rslade@sprint.ca>  
Tue, 16 Oct 2001 11:57:29 -0800

[I think this book is very much worthy of mention in RISKS, despite the identity of the reviewer. PGN]

BKVR.RVW 20011013

"Viruses Revealed", Robert M. Slade/David Harley/Urs Gattiker, 2001,  
0-07-213090-3, U\$39.99  
%A Robert M. Slade rslade@sprint.ca, rslade@vcn.bc.ca, pl@canada.com  
%A David Harley harley@sherpasoft.org.uk, macvirus@dircon.co.uk  
%A Urs Gattiker (Denmark)  
%C 300 Water Street, Whitby, Ontario L1N 9B6  
%D 2001  
%G 0-07-213090-3  
%I McGraw-Hill Ryerson/Osborne  
%O U\$39.99 905-430-5000 +1-800-565-5758 fax: 905-430-5020  
%P 700 p.  
%T "Viruses Revealed"

The International Institute for Fashion and Other Really Nasty Things today announced the winner of the 2001 Award for the World's Ugliest Book Cover. "Normally, we wouldn't announce a winner until next spring some time," said Frederick Krueger, the Institute's president, "but with the release of `Viruses Revealed,' there really isn't room for any competition."

Spokespeople for Osborne/McGraw-Hill would not speak for attribution, but one did admit that they were pleased with the award. "We said we were going for 'bold' and 'eye-catching,' but our real target was to produce that sick-to-your-stomach flu feeling, to give people a real virus queasiness. It's nice to know we succeeded."

Security specialists were equally quick to comment on the contents of the work. "What a thick book!" said David Chess.

"Da- I mean, darn it, where are the taxonomies?" said Winn Schwartau, author of "Internet and Computer Ethics for Kids." He also promised to give us his \*real\* reaction "as soon as I get rid of the best of these rugrats."

"I think more time should go by between Slade's books." - Larry Bridwell

"How come my work didn't get mentioned?" - sarah gordon

"read it" - A. Padgett Peterson

"Should be 'reviled'." - PGN

"A mythic work! No, sorry, that should be 'mythical'." - Jeff Crume

"Why are these guys misusing my name?" - Gene Spafford

"Makes a great doorstop." - Tom Sheldon

"Oooh, a foreword from spaf!" - David Chess (no relation)

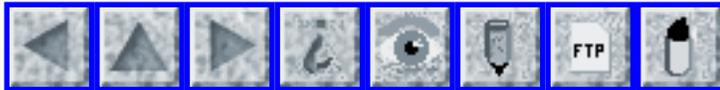
"Fills an unneeded gap." - Fred Cohen

Misinformation about semi-recent viruses can be found at

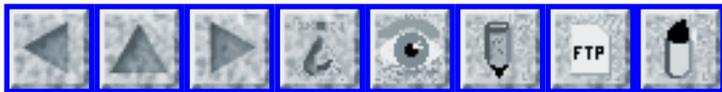
[http://www.osborne.com/virus\\_alert/](http://www.osborne.com/virus_alert/), while marketing hype is available at <http://victoria.tc.ca/techrev/vrupdate.htm> and <http://sun.soci.niu.edu/~rslade/vrupdate.htm>. Some real links can be found at <http://www.sherpasoft.org.uk/viruses-revealed/>.

copyright Robert M. Slade, 2001 BKVR.RVW 20011013  
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 21: Issue 71**

**Weds 24 October 2001**

## Contents

- [With Mars probe maneuver, NASA finally catches a brake  
inthenews](#)
- [DB and WWW on one machine in Australian election  
Andrew Goodman-Jones](#)
- [Web defacement and cyberattacks  
Dave Stringer-Calvert](#)
- [Hacker cracks Microsoft anti-piracy software  
Monty Solomon](#)
- [Are spammers getting sneakier? part 1  
Rob Slade](#)
- [Are spammers getting sneakier? part 2  
Rob Slade](#)
- [Redesi virus  
Rob Slade](#)
- [The British BSE crisis  
Anthony W. Youngman](#)
- [Pregnant chad revisited  
Fred E. Ballard](#)
- [Re: Stray bomb caused by typo  
Dan Jacobson](#)

- [Non-risk, re: Jet engine starter motors](#)  
[Ben Laurie](#)
  - [Re: Euro changeover](#)  
[Otto Stolz](#)
  - [Re: Improper address-change validation](#)  
[Chuck Falconer](#)
  - [Cutting through hype, spin, and propaganda - "Fact Squad Radio"](#)  
[Lauren Weinstein](#)
  - [Re: Ham radio and Morse Code](#)  
[Scott K. Ellis](#)  
[Skip La Fetra](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

## ✶ **With Mars probe maneuver, NASA finally catches a brake**

inthenews <inthenews@SIGMAXI.ORG>

Wed, 24 Oct 2001 11:11:44 -0400

[In RISKS, we try to include success stories, not just catastrophes. Here

is a NASA success (albeit after several Mars-related failures that have

been reported here earlier). This item is from \*The Washington Post\*,

23 Oct 2001, via Science In the News (Sigma Xi). PGN]

The Mars Odyssey, which left Earth seven months ago, braked into orbit

around the red planet last night, giving NASA's Mars program a welcome boost

after back-to-back failures in 1999. While outwardly confident, engineers

at NASA's Jet Propulsion Laboratory in Pasadena, Calif., were anxious about

the make-or-break "Mars orbit insertion" -- MOI -- rocket firing, a

19.7-minute maneuver one manager described as "the longest 20

minutes of our lives." In reality, engineers had to wait a full half-hour to find out whether Odyssey's main engine had done its job. After a brief scare caused by a momentary loss of data, flight controllers were able to confirm the rocket firing had started on time at 10:26 p.m. EDT based on analysis of radio transmissions from the spacecraft. But Odyssey disappeared behind Mars -- as expected -- halfway through the maneuver.

<http://www.washingtonpost.com/wp-dyn/articles/A42061-2001Oct23.html>

---

## **DB and WWW on one machine in Australian election**

"Andrew Goodman-Jones" <goodie@ozemail.com.au>

*Mon, 22 Oct 2001 15:17:52 +1000*

Technical hiccups hit ACT election counting

By Sandra Rossi, 22 Oct 2001, Computerworld Australia

It is ironic that counting in Australia's first election offering electronic voting stalled because of technical hiccups following the ACT poll [on 20 Oct 2001]. Electronic voting is supposed to speed up the polling process and was used on Saturday during the ACT election offering voters a choice between traditional paper ballots and the Internet. By the time voting closed, the ACT Electoral Commissioner Phil Green was claiming Internet users significantly slowed down the collating of electronic votes.

More than 11,000 pre-poll electronic votes were supposed to have been counted just after the polls closed at 6pm but there were periods when counting was at a virtual standstill. According to Green, disks were slower to load than expected and processing the disks for eight polling stations equipped for computer voting was drawn out because of competition from the Internet. "We're getting lots of hits on our Internet site and that's actually slowing down our server because it's all being run off the one database," Green said during counting.

<http://www.computerworld.com.au/IDG2.NSF/a/00046162?OpenDocument&n=e&c=CP>

---

## 🔥 Web defacement and cyberattacks

Dave Stringer-Calvert <dave\_sc@csl.sri.com>  
*Mon, 22 Oct 2001 17:37:08 -0700*

GForce Pakistan hackers defaced the U.S. Defense Test and Evaluation

Proccessional Institute Web site [www.dtepi.mil](http://www.dtepi.mil) as well as [enduringfreedom.dtepi.mil](http://enduringfreedom.dtepi.mil) and [nasa.dtepi.mil](http://nasa.dtepi.mil)

<http://www.newsbytes.com/news/01/171341.html>

after which a rival group of Pakistani vigilante hackers (Yiyat) identified

the purported culprit and retaliated.

<http://www.newsbytes.com/news/01/171365.html>

[Above text PGN-ed from the URLs. I tried to verify the "proccessional", but [dtepi.mil](http://dtepi.mil) was apparently off the Net. PGN]

Also, an interesting CNN article on a DoE cyberattack scenario.  
Best  
quote:

The important lesson is that Black Ice showed how interdependent are the various infrastructure systems -- including telecommunications, utilities and banking -- and how major might be the combined effects of cyber- and physical attacks, she says.

The infrastructure system providers didn't understand the interdependencies among their systems," Scalingi says. "If you talk to state and local government and local utilities, they'll tell you they have great response plans. The problem is, they write them in isolation.

<http://www.cnn.com/2001/TECH/ptech/10/21/black.ice.idg/index.html>

---

## **🔥 Hacker cracks Microsoft anti-piracy software**

Monty Solomon <monty@roscom.com>  
*Sun, 21 Oct 2001 01:45:01 -0400*

By John Borland, Staff Writer, CNET News.com, 19 Oct 2001

A piece of software being distributed anonymously online has successfully cracked part of Microsoft's anti-piracy technology, the centerpiece of much of the giant's recent forays into the audio and video world.

Microsoft confirmed Friday that the code, written by a programmer using the pseudonym "Beale Screamer," can strip off the protections that

prevent a  
song from being copied an unlimited amount of times.

The company's digital media division has spent much of the day talking to record labels and content partners in an effort to respond to Screamer's software, said Group Product Manager Jonathan Usher.

<http://news.cnet.com/news/0-1005-200-7590303.html>

---

## **✶ Are spammers getting sneakier? part 1**

Rob Slade <rslade@sprint.ca>  
*Fri, 19 Oct 2001 09:33:54 -0800*

As we are all well aware, spam has been around for a while. As most of us are aware, replying to the "if you have received this message in error and want to be removed from our lists" message at the bottom of most spam simply allows the spammers to verify that they have a "live one"--e-mail address, that is.

Recently I received a flood of spam, all simply offering to take my name off their list--if I replied to it. I guess the clients of spam companies are starting to get pickier about the quality of the lists.

However, I have also started to receive the odd message like one I got this morning. The subject line stated that the sender saw my ad on Google. Now, I don't advertise on Google. But then again, Google is a Web search tool,

and a lot of people are careless about differentiating between the vast quantities of sites out there consisting solely of masses of banners, and information sites like the ones I have up. Reading the message was no more informative: it simply asked me to send more information.

The headers were more interesting. The message was ostensibly from someone at referralware.net, but the "Received" lines indicated an origin at prontomail.com.

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>

---

## ✂ Are spammers getting sneakier? part 2

Rob Slade <rslade@sprint.ca>  
*Sun, 21 Oct 2001 22:01:45 -0800*

So I get this e-mail with no subject, but the "From" name is the same as my daughter. Only, of course, it isn't her. It's somethingtosell15678@aol.com. Only it isn't that, either, when you look at the headers, it's:

```
Received: from Azzarmaster (ppp-178.11.triton.net  
[216.65.178.11] (may be forged))
```

Now isn't that clever! triton.net has determined that the header information \*it\* received may be forged! It is helpfully warning me that I may be receiving spam! Really? How would it know? Is this, perhaps, an

open relay? And, if so, why is it open? Why isn't triton.net closing off this type of abuse?

Well, let's look at the IP address, 216.65.178.11. Good old Samspace.org can tell us that:

Trying whois -h whois.arin.net 216.65.178.11

```
Lucre, Inc. (NETBLK-LUCRE)
  4011 Plainfield Ave
  Grand Rapids, MI 49525
  US
```

[...]

```
Coordinator:
```

```
  Hale, Steve (SH1448-ARIN)  steve@lucre.net
  (616) 361-0128
```

OK, lucre.net certainly sounds like a domain name that a spammer would pick.

However, the information goes on:

Domain System inverse mapping provided by:

```
NS1.TRITON.NET 209.172.0.5
```

So let's be guessing that the header isn't actually forged at all. Perhaps we are just supposed to give up looking when we see an indication of a forged header, and not try to find out who actually sent this message. Or, perhaps triton.net is simply going for plausible deniability: "Spam? Gee, that's too bad. Bummer that the headers are forged, otherwise we could tell who sent 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>

## ⚡ Redesi virus

Rob Slade <rslade@sprint.ca>

*Sun, 21 Oct 2001 11:44:54 -0800*

RISKS readers may have heard of one or both variants of Redesi, also known as Dark Machine or Ucon. (In fact, it was PGN who first alerted me to the existence of the second.) (If you haven't heard about them, don't open any e-mail attachments with filenames of Common.exe, Rede.exe, Si.exe, UserConf.exe, or Disk.exe. These filenames seem to be consistent in both versions, in file attachments, and on infected machines.)

There are two variants. One comes with a large variety of possible subject lines, all of which contain either a double hyphen or an ellipsis (three or six periods). Many appear to be comments from Kev, Gaz, Will, Si, Jim, Arwel, or Michelle. The body of the message of this A version reads "heh. I tell ya this is nuts ! You gotta check it out !" and file attachments with filenames as listed above. Infected machines will have files with the filenames listed created in the root directory of the C: drive with the hidden attribute set. However, this variant doesn't make any changes to the Registry, and doesn't do any apparent damage.

The second variant comes with a subject line that may refer to Microsoft, security updates, alerts, terrorists, emergency response, and

viruses. The body contains what appears to be a message from Microsoft describing the attachment as a security patch, and a message of endorsement from the forwarder. (Since both variants are forwarded using Microsoft Outlook address books, the messages will appear to come from someone you know.) (Note that Microsoft is not in the habit of sending out security patches as e-mail attachments.) The B variant adds entries to the Registry, and attempts to use an entry in the Autoexec.bat file to reformat the disk on or after November 11, 2001. The filenames of the attachments, and the files created, are the same.

Note that the close association and quick release of the two variants may have been a two stage piece of social engineering. The first release would create some concern, and would promote a heightened sense of urgency about applying patches or fixes, possibly enough to prompt people to run suggested repair programs without getting confirmation. The second virus would take advantage of this kind of panic. And, in this case, the "cure" is definitely worse than the disease.

(However, given some of the second set of subject lines, the second release may simply be trying to take advantage of the uncertainty over terrorist attacks.)

By the way, if you are trying to filter viruses at the e-mail gateway, scan e-mail for messages with attachments with filenames Common.exe, Rede.exe,

Si.exe, UserConf.exe, or Disk.exe. Also note the message text "heh. I tell ya this is nuts ! You gotta check it out !" and "Just recieved this in my email I have contacted Microsoft and they say it's real !" Note that deleting messages on the basis of body text is not recommended, since it may eliminate warning messages.

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>

---

## **✶ The British BSE crisis**

"Anthony W. Youngman" <Anthony.Youngman@ECA-International.com>  
*Mon, 22 Oct 2001 15:08:30 +0100*

[This message is not particularly relevant to COMPUTERS,  
but highly relevant to TRUSTING THIRD-PARTIES. PGN]

As you probably know, some scientists were asked to study whether BSE had jumped species into sheep, and were given a load of sheep-brains to study. It then turned out that these were not sheep, but cow brains, leading to newspaper headlines about how scientists couldn't tell the difference between sheep and cows.

This morning, it took a turn for the worse. It appears that the scientists \*had\* suspected something was wrong, and asked for a sample of their material to be analysed to check the species. However, as their

brief was to look for BSE, they could only \*request\* that somebody else check for species. It seems that when this check was done, it was done on a sample of material that the original scientists \*should\* have been given, not on the sample they had provided from what they \*had\* been given. So of course the species test "proved" they had sheep brains.

The risk? The classic "need to know" principle meaning that people are forced to rely on others "doing the right thing" rather than being empowered to make sure themselves that things are okay. And the classic of basing your test on the assumption that things are okay, rather than assuming (and looking for) a cock-up. [Heard on Radio 4]

---

## **✶ Pregnant chad revisited (Re: Jones, [RISKS-21.70](#))**

<fred.e.ballard@abbott.com>

*Mon, 22 Oct 2001 11:32:18 -0500*

It is shocking that a risk so obvious was not mentioned or found. I think it is a real insult to voters, and a disgrace to the manufacturer and voting officials.

Sheesh! Like so many things in RISKS, an intelligent sixth grader wouldn't run things this way.

Fred Ballard   fredb@acm.org   fred.ballard@abbott.com

[The really sad thing is that many of the same punch-card machines

were apparently also implicated in the 1988 Florida Senate race.

Buddy Mackay lost a close election to Connie Mack, in which there was

a drop-off of 210,000 votes relative to the Presidential race in the

same four counties. A lot of people must have been asleep at the wheel.

PGN]

---

## ✶ Re: Stray bomb caused by typo (Hollebeek, [RISKS-21.70](#))

Dan Jacobson <jidanni@deadspam.com>

20 Oct 2001 08:19:35 +0800

> ... GPS coordinates could use a check digit that detects one digit errors

> and transpositions, much like the one used in credit-card numbers.

Erm, but aren't any coordinates valid as long as you don't go beyond, e.g. 90 degrees north latitude, etc. OK, yes, it would be wise to check that the coordinates are indeed within Afghanistan, unless oops, we want to create a random international incident, or maybe even blow ourselves up.

Odd that with all that high tech, he still had to type them in instead of clicking on it...

Or maybe he needs an Afghanistan Residential Zoning Map hooked into his GIS to lock out bad picks.

<http://www.geocities.com/jidanni/> Tel+886-4-25854780 ǝnα|¥§

[Also commented on by Lou Schneider. PGN]

---

## ✶ Non-risk, re: Jet engine starter motors ([RISKS-21.70](#))

Ben Laurie <ben@algroup.co.uk>

*Sun, 21 Oct 2001 21:28:46 +0100*

One of the rays of sunshine in the otherwise bleak cloudspace that is RISKS is that the occasional risk turns out not to be. I have been told by a significant number of people that the starter motor is not what goes on "continuous" after the jet has taken off. Instead the ignitors stay on and ensure that if the flame goes out, it is relit. It is, apparently, normally not necessary to respin the turbines once in flight.

If I remember correctly, because the 777's engine start sequence is entirely automated (literally one switch for each engine), there's no distinction made between starter motors and ignitors on the control panel. There's a single switch that does, in effect, "off", "on" and "continuous".

Thanks for all the corrections on this issue.

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

---

## ✶ Re: Euro changeover (Long, [RISKS-21.70](#))

Otto Stolz <Otto.Stolz@uni-konstanz.de>

Mon, 22 Oct 2001 19:38:57 +0200

On Sun, 14 Oct 2001 21:50:48 +0200, Douglas Long wrote:

> Converting all values to Euros and then calculating the  
> account balance [...] yields one answer. Calculating a  
> partial balance in Francs, converting to Euros, and then  
> completing the remaining calculations using Euros [...]   
> yields a slightly different result.

This is an intrinsic property of the two operations {conversion  
| addition}:

they are not commutative;

cf. <<http://europa.eu.int/euro/html/dossiers/00121/00121-en.pdf>>.

Hence, there are rules the banks are legally bound to,

cf. <<http://europa.eu.int/euro/html/home5.html?lang=5>>.

However, according to the dossier cited above, the particular  
issue observed by Douglas Long is subject to national rules.  
[...]

(Note: EUR cash will only be introduced on 01 Jan 2002)

> some ATM transactions are reported in Francs ... others ...  
in Euros

This sort of happening is forbidden in Germany. However, I do  
not know  
anything about national regulations in France.

In Germany, customers currently can choose whether their  
accounts are  
handled in DM or in EUR. Banks are committed to carry the  
original amount  
and currency of every single transaction through to the final  
account (in  
addition to the EUR amount they use for their own balancing);  
hence, if a DM  
amount is transferred from one DM account to another DM account,  
the

original DM amount will precisely be balanced in both customer accounts, notwithstanding the fact that the banks themselves calculate in EUR. The same scheme applies to cash deposits to, and withdrawals from, DM accounts.

---

## ✂ Re: Improper address-change validation

CBFalconer <cbfalconer@yahoo.com>

*Sat, 20 Oct 2001 03:18:24 GMT*

The US postoffice operates the same way. I recently put in a change of address, and the advisory went to the new address, along with all the old mail.

Chuck F (cbfalconer@yahoo.com)

[At SRI, we did a study for the USPS many years ago, and I complained

then about that stupid policy. Evidently, they still have not learned. PGN]

---

## ✂ Cutting through hype, spin, and propaganda - "Fact Squad Radio"

Lauren Weinstein <lauren@vortex.com>

*Wed, 24 Oct 2001 10:42:25 -0700*

Announcing "Fact Squad Radio"

October 21, 2001

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

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

[ To subscribe or unsubscribe to/from this list, please send the command "subscribe" or "unsubscribe" respectively (without the quotes) in the body of an e-mail to "pfir-request@pfir.org". ]

Greetings. The main purpose of People For Internet Responsibility's recently-announced "Fact Squad" effort is to cut through hype, spin, misinformation, and propaganda regarding technological issues and their effects upon society.

In furtherance of this goal, we're pleased to announce the launching of the "Fact Squad Radio" service. Fact Squad Radio is providing very short (one minute), tightly-focused audio features, each concentrating on a single relevant topic of importance. These vignettes are aimed at explaining the issues briefly in a non-technical manner suitable for general audiences. Topics to be covered will include both matters of long-standing importance and crucial issues of the moment.

We encourage linking and redistribution of these features, and they are freely distributable without any further permission being needed for non-broadcast, non-commercial usage. Requests for other kinds of usage will be considered on a case-by-case basis. We'll be ramping up towards a five per week, M-F schedule. All segments are in the standard MP3 format.

The debut Fact Squad Radio feature concerns a topic of some significant interest right now -- National ID Cards.

Fact Squad Radio is at:

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

Thanks very much!

Lauren Weinstein [lauren@pfir.org](mailto:lauren@pfir.org) [lauren@vortex.com](mailto:lauren@vortex.com)

[lauren@privacyforum.org](mailto:lauren@privacyforum.org)

Tel: +1 (818) 225-2800

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

Co-Founder, Fact Squad - <http://www.factsquad.org>

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

Member, ACM Committee on Computers and Public Policy

---

## ✶ Re: Ham radio and Morse Code (Decker, [RISKS-21.70](#))

"Scott K. Ellis" <[storm@stormcrow.org](mailto:storm@stormcrow.org)>

*Fri, 19 Oct 2001 21:43:40 -0400*

With due respect to Mr. Decker, I believe he has slightly (perhaps unintentionally) distorted the most recent developments in amateur radio licensing. While it may be true that the ham radio community has in the past considered Morse code a "favorable" barrier to entry to keep out "undesirables," current Morse code requirements have a more reasonable explanation. The maximum required Morse code speed for a ham license is now 5 WPM. While there are several license grades with more "long

distance"  
frequency bands available for use, they are now all accessible  
by passing  
the appropriate technical knowledge test. The 5 WPM code  
requirement for  
the long-range frequency bands is a result of international  
treaty  
requirements. There are currently efforts underway to have that  
portion of  
the international treaties changed, at which time the Morse code  
requirement  
will be removed from the amateur licensing requirements.

Scott K. Ellis

---

## ✶ Re: Ham radio and Morse Code (Decker, [RISKS-21.70](#))

"Skip La Fetra" <Skip@LaFetra.com>

*Sat, 20 Oct 2001 10:35:12 -0700*

> ... And it's also something that could come back to bite you  
in the butt,  
> should those of the "excluded" class ever reach positions of  
power.

No truer words have ever been spoken. Mr Decker's points  
against the Morse  
code requirement are true and to-the-point (I speak as an  
Amateur Extra (20  
words-per-minute Morse) licensee who has *\*never\** attempted a  
"real" Morse  
contact -- I learned the code (and it *\*IS\** very hard!) simply to  
get the  
license. Mr. Decker's points about exclusion ring true.

However, there are other points which were omitted in his  
message which need  
to be made in balance -- and this is my reason for this message

to RISKS.

These are not "rebuttals" to his premise, but point to other reasons why

Amateur ("ham") radio is justified in today's society.

Ham Radio (and its FCC justification) is about COMMUNICATION.

We are a

trained bunch of COMMUNICATORS (it does not really matter if we are using

Ham, CB, or other frequencies) who are experienced at accurate COMMUNICATION. We are equally skilled at picking up a police or fire

hand-held radio as we are at using our "special" frequencies -- and getting

a CLEAR message across. In an emergency situation, communication needs far

outstrip the installed capability -- Hams are PEOPLE who have frequencies

(communication channels) and clear-communication skills who can use their

resources (or those of the police/fire/Red Cross agency they are present to

help) to keep information flowing. (I do wish to point out that the ham

"special" frequencies are necessary to augment the limited number of

police/fire channels in a true communications emergency.)

This is (one of) the core justification(s) of Ham radio by the FCC. Active

(hobby) use of the radio spectrum enables ham operators to be ready and able

to help in times of communications emergency. Morse Code is a useful

method, but it is not the only method.

Skip La Fetra, Amateur Extra, AA6WK, Skip@LaFetra.com

<http://www.LaFetra.com/Skip/AA6WK>

[I have omitted several other messages on this topic, but there seems to be lively disagreement. 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 21: Issue 72**

**Tuesday 30 October 2001**

## Contents

- [TD Bank Canada system crash](#)  
[Richard Akerman](#)
  - [ANOTHER SRI-wide Power Outage](#)  
[PGN](#)
  - [ACT Election Electronic Voting](#)  
[Josh Polette](#)
  - [Project Liberty](#)  
[Jay R. Ashworth](#)
  - [Re: Are spammers getting sneakier?](#)  
[Crispin Cowan](#)
  - [Re: Are spammers getting sneakier? - Yes, they are](#)  
[Greg Searle](#)
  - [USPS correction](#)  
[Ken](#)
  - [NSF Trusted Computing program](#)  
[Carl E. Landwehr](#)
  - [REVIEW: "Malicious Mobile Code", Roger A. Grimes](#)  
[Rob Slade](#)
  - [Info on RISKS \(comp.risks\)](#)
-

## **TD Bank Canada system crash**

Richard Akerman <rakerman@chebucto.ns.ca>

*Tue, 30 Oct 2001 09:53:43 -0400 (AST)*

This past weekend in Canada, one of our 5 major banks, the Toronto-Dominion, experienced a serious systems failure. This caused particular problems because Canadians use debit cards more than any other nation, in fact, many people (including me) carry only a debit card and credit card in their wallet, and no cash.

The Tuesday, October 30, 2001 *\_Globe and Mail\_* reports in "TD aims to clear backlog following system crash" that:

'The crash was caused by the failure of a single "motherboard" in one of the bank's central computers at about 11 a.m. Saturday [Oct 27, 2001].

This "gradually started to shut down the system" to "protect the integrity" of the data already there, Mr. Livingston [head of TD electronic banking] said.'

Then this remarkable statement

'It was a purely random event," he said, adding that hardware failures are rare. "This has never happened before, and it will likely never happen again."'

and ending with

'As TD sought to identify and fix the problem, "a few million transactions" were rejected by the bank's systems, which, on a

busy

Saturday, process up to 500 transactions a second, he said.

The bank's computer systems have all sorts of "redundancies" built in to try to protect against failures, but the incident on Saturday "just shows you can't protect against the random element," Mr. Livingston said.'

This seems to me to be a remarkable design philosophy.

Richard J. Akerman <rakerman@chebucto.ns.ca>

<http://www.chebucto.ns.ca/~rakerman/>

---

## **✶ ANOTHER SRI-wide Power Outage**

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

*Sat, 27 Oct 2001 13:45:33 -0700*

Despite our carefully conceived phased UPS systems, standby generators, and co-generation plant designed to keep SRI in continuous power, we experienced a site-wide power outage Saturday morning that took everything electrical down with it.

Thanks to Dave Stringer-Calvert for sharing the punch-line from an SRI facilities memo:

"The power outage was caused when Cogen staff pressed the wrong button and took the facility off-line."

## **ACT Election Electronic Voting**

<joshpolette@ozemail.com.au>

Thu, 25 Oct 2001 19:54:31 +1000

The recent ACT Assembly Elections created a first in Australian political history by introducing electronic voting. It was not a full scale implementation with electronic voting limited primarily to pre-poll voting and to a small number of polling stations on election day. Electronic voting was intended to provide great benefits in vote counting because of the complexity of the Hare-Clark system. However, this was not to be. There was a flaw in the architecture of the system. The system was designed to allow live results to be viewed on the Internet. Unfortunately, the same server that was doing the number crunching (ie, counting the votes) was also the one serving information to the Internet. As a result, the rate of vote counting was severely impacted by the load placed on the server by voters eager to see the results.

URL: [http://news.ninemsn.com.au/Sci\\_tech/story\\_20717.asp](http://news.ninemsn.com.au/Sci_tech/story_20717.asp)

There are several causes for concern in this article, primarily because of the sensitivity of the subject (ie, election vote counting). After the fiasco in the US Presidential elections over ballot paper design and counting, there was a call for electronic voting to be introduced. The theory being that computers are never wrong. However, the ACT experience

shows that it is not guaranteed. While there is no evidence that vote tampering has occurred it is of concern that Internet activity can affect the counting process of an election. Surely, the counting system should be isolated from the Internet with only a copy of the interim results stored in a separate, Internet accessible server? What is really worrying is that the article doesn't say whether the actual web server was running on the vote counting server or not. Given the severe impact on counting performance, one has to wonder.

Josh Polette, Engineering Manager, JCSS, ADI Limited, C4ISR, IS3  
Phone: 02 6247 6854 Fax: 02 6247 7864 joshpolette@ozemail.com.au

---

## Project Liberty

"Jay R. Ashworth" <jra@baylink.com>  
*Tue, 23 Oct 2001 14:17:16 -0400*

In last week's Linux Weekly News, there was some preliminary coverage of Project Liberty, an "open" alternative to Microsoft's Hailstorm, which is -- very roughly -- an attempt to embed Passport into everything on the planet.

The short version is: a repository of information about your person, life, and preferences which can be accessed by people and companies you authorise, to provide authentication that you are you, and information about, for

example, your purchase default desires (credit-card numbers, which card to use, do you prefer first class or coach, etc).

Now, this is, fundamentally, not an especially bad idea.

But how it is implemented is -- given the sort of information which it might end up holding -- pretty crucial to your personal privacy: do you want anyone except your doctor and your pharmacist knowing that you have a prescription for protease inhibitors? (Drugs used to control AIDS and related conditions.)

You probably don't even want your \*health insurer\* to know that, even though perhaps you want them to know \*other\* things about you, and therein lies the major problem:

Hailstorm will be run by Microsoft.

And we all know how pristine Microsoft's track record is for placing the interests of individuals above that of large corporations off of whom Microsoft makes lots of money. Right?

So here comes Project Liberty, an "open" alternative to this. They've not much design done yet, I don't think, so we don't know what \*specific\* goals PL will be aiming towards. But that's good, because it means that this is the exact time for private individuals to be casting their bets on what they think is important: personal privacy and control are good choices there, IMHO.

I know that in our New World, it's almost unpatriotic to be

concerned about  
personal privacy, but you know what? That's a wrongheaded,  
short sighted,  
and dangerous outlook to have. Our country became something to  
be proud of,  
protect, and defend precisely *\*because\** it attempted to secure  
such  
liberties to the people against government control, and  
corporations should  
be given no extra leash -- they work for *\*us\**, in the final  
analysis, just  
like the government.

But the most fundamental tenet of Project Liberty's operation  
must be, for  
it to succeed, that it will always favor the desires and  
interests of those  
one billion people whose identities it likes to tout it's  
representation of  
*\*over\** the interests of the corporations with all the money.

>From a design standpoint, it must make it possible to break  
down your  
information to a sufficiently fine granularity to allow you to  
authorize  
access for someone to only the data which you want them to  
have... and  
indeed, to make it as difficult as possible for different  
providers to  
cross-correlate the information they hold privately about you  
with one  
another. (Why do I get my cablemodem service from one company,  
my wireless  
Internet from someone else, and my cellphone service from yet  
another  
company? Because I *\*can\**, and because if one bill is late, I  
don't get cut  
off from all three. Do I want to give that flexibility up?  
Certainly not.)

Ensuring that the provision of the convenience of "single-sign  
on" won't  
deprive me of rights and conveniences I now have won't

necessarily be easy  
for the Project Liberty folks.

But if they don't do it, and stick to it, then I will not -- and  
you should  
not -- give them any more quarter than Microsoft. Regardless of  
whom they  
have on their side.

Jay R. Ashworth, Member of the Technical Staff Baylink, The  
Suncoast Freenet  
Tampa Bay, Florida <http://baylink.pitas.com> +1 727 804 5015  
jra@baylink.com

---

## ✶ Re: Are spammers getting sneakier? (Slade, [RISKS-21.71](#))

Crispin Cowan <crispin@wirex.com>  
*Fri, 26 Oct 2001 16:43:10 -0700*

The "may be forged" note is a standard indication from the MTA  
(Mail  
Transfer Agent, i.e., mail server) that the host the MTA is  
receiving this  
mail from cannot successfully be reverse-DNS'd. If the MTA did  
reverse DNS  
on the originating IP and got a different name, it would have  
told you that.  
As it is, it is just saying that it doesn't trust the claim that  
this is  
from triton.net.

Given the fairly prolific amount of inaccurate reverse DNS info  
out there,  
this isn't even a reliable indication that a give piece of e-  
mail is spam.  
But in the context that Slade provides (multiple forged headers,  
stupid  
generic query) it is a good bet.

I've seen it many, many times in the last couple of years of spam-fighting. The earliest instance I have a record of is August 1998, but that's only because that is literally the oldest archived spam that I have. Since then I have logged approximately 2000 occurrences of such spam. An interesting result of this investigation: the frequency has dropped sharply in recent years, although spam frequency certainly has not. Whatever spam technique causes this to occur appears to be falling out of favor.

Crispin Cowan, Chief Scientist, WireX Communications, Inc.

<http://wirex.com>

Security Hardened Linux Distribution: <http://immunix.org>

---

## ✶ Re: Are spammers getting sneakier? - Yes, they are

"Greg Searle" <greg\_searle@hotmail.com>

*Fri, 26 Oct 2001 12:28:45 -0400*

Here's the bag of tricks that many spammers are using to keep you from finding out who really sent you the spam:

1. The obvious - find an open e-mail relay, and use it for "e-mail laundering". Forge the e-mail headers, and the e-mail becomes untraceable.

All you see is the IP for the open relay, and whatever the spammer wants you to see afterward. The "From" header is always forged, and complaining to the ISP behind the "From" address is pointless. The most you can do is

complain to the company that owns the open relay, and hopefully they will close it. Unfortunately, new mail servers appear on the net every day, and many IT "professionals" setting up these systems are just not aware of the open relay problem. There are many web pages which have the sole purpose of finding and listing these open relays.

2. Include a "relay" URL in the spam for potential customers. This URL is typically a "throwaway" account opened on one of the many free webpage services (tripod, geocities, angelfire, etc.) with false credentials. The spammer only expects this URL to exist for a day or two, as the provider will quickly terminate the page once complaints start coming in. The URL typically points to a file or page that will redirect the customer to the true page.

3. There are some businesses that are specifically set up to relay URLs for spammers. One of these is 1freesite.net (G Stubberfield Enterprises). Spammers hire the business to set up a relay page on their server, so they can include this page in their e-mails.

4. Obfuscate the URL in an attempt to make it untraceable. Do you know that IP addresses can be expressed as a single, decimal digit? Browsers will accept this digit and translate it into a valid IP address. Encoding the URL in hex is another trick. Browsers will convert two-digit hex digits that are preceded by a percent sign into a valid character. The URL specification also allows usernames and passwords in a URL.

This can be used to mislead. For instance, the URL <http://www.webservice.com:www.server.com@192.168.10.10/spampage.html> seems to point to "webservice.com", but the piece of the URL before the second colon is really the "username", the piece before the at sign is the "password", and the real web server is the IP after the at sign! Most web servers simply ignore the user name and password if they don't need it. These techniques can be combined to make a URL really hard for a person to decode.

5. Compose the relay webpage in JavaScript. Encrypt the "real" web page and any URL's, and have a JavaScript function decode it.

6. Ask customers to respond to the message. Include a valid "Reply To" header that is different from the "From" header. The e-mail client will recognize this and send any responses to the "Reply To" address. The e-mail account set up to receive these messages is usually a "throwaway" address set up on a free mail service with false credentials.

7. Include an unlisted phone number, which is protected by the telephone company and is untraceable.

8. Included an executable at the URL enclosed in the message. This executable is typically compressed to obfuscate its contents from prying binary file editors. The executable then forwards the customer's computer to the business's true URL. Anybody who opens this executable file is too ignorant to know any better.

All of these methods, except for the telephone number and the reply-to address, are completely reversible to expose the company behind the e-mail. If the computer can get to the final page, then so can the person operating the computer, given enough knowledge of the technology involved. There is one particularly nasty spammer, hosted at sexmansion.com and web69.com, that includes a doubly-compressed executable in the page that they set up on a "throwaway" site. Their extremely explicit e-mailings point to this executable's URL. This executable is a dialer application that redirects the user's modem to an offshore telephone number and sends their browser to one of the above mentioned domains. This appears as a charge on their telephone bill. This business was rather clever with the obfuscating technology used to hide their presence, but the same technology can be used to unravel the obfuscation and find the business behind it.

---

## **✶ USPS correction (Re: Improper address-change validation)**

Ken <kenzo@free-music.com>  
*Wed, 24 Oct 2001 22:30:54 -0400*

>... the advisory went to the new address, along with all the old mail.

Actually, their policy is slightly better than this; they send advisories to both the old and the new addresses. So, in theory, you can rush to the post

office upon receiving the advisory and at least stop them from forwarding any additional mail. Not terribly secure (no attempt is ever made to verify your identity), and it depends on you successfully receiving the advisory, but it's still slightly better than cutting your old address off altogether.

kenzo@free-music.com

[... but not much help if you are away for a month. PGN]

---

## **✶ NSF Trusted Computing program**

"Landwehr, Carl E." <clandweh@nsf.gov>

*Thu, 25 Oct 2001 14:56:01 -0400*

[Carl Landwehr, erstwhile security guru at the U.S. Naval Research Lab and

more recently at Mitretek, is now on a one-year leave at the National

Science Foundation, as Director of the Trusted Computing program. NSF is

a good source of funding, and this procurement should be of interest to

many RISKS readers. As always, I recommend that we focus on developing

TRUSTWORTHY systems, not just UNTRUSTWORTHY systems that have to be

TRUSTED because we have no alternative. PGN]

The initial announcement for the new Trusted Computing program is at:

<http://www.nsf.gov/pubs/2001/nsf01160/nsf01160.html>

The deadline for proposals is 5 Dec 2001; if you are in a position to

conduct research in this area, I encourage you to consider submitting a proposal. 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 new contact information is provided below; please use this e-mail address for future correspondence.

Carl E. Landwehr, Program Director, Trusted Computing, CISE/CCR, Suite 1175  
National Science Foundation, 4201 Wilson Blvd., Arlington, VA 22230  
e-mail: [clandweh@nsf.gov](mailto:clandweh@nsf.gov) phone: 703-292-8936 fax: 703-292-9059

---

## **REVIEW: "Malicious Mobile Code", Roger A. Grimes**

Rob Slade <[rslade@sprint.ca](mailto:rslade@sprint.ca)>  
*Mon, 29 Oct 2001 08:00:43 -0800*

BKMLMBCD.RVW 20010814

"Malicious Mobile Code", Roger A. Grimes, 2001, 1-56592-682-X, U\$39.95/C\$59.95

%A Roger A. Grimes [roger@rogeragrimes.com](mailto:roger@rogeragrimes.com)  
%C 103 Morris Street, Suite A, Sebastopol, CA 95472  
%D 2001  
%G 1-56592-682-X  
%I O'Reilly & Associates, Inc.  
%O U\$39.95/C\$59.95 800-998-9938 fax: 707-829-0104 [nuts@ora.com](mailto:nuts@ora.com)  
%P 522 p.  
%T "Malicious Mobile Code: Virus Protection for Windows"

I have to admit to a very definite bias. My co-authors and I have just finished a book that attempts to provide up to date virus

protection

information to sysadmins. As I understand it, ours will be printed about three weeks after this one.

I also have a problem with the title. Grimes appears to be trying to carve himself out a niche by promoting a term that nobody else is currently using.

And the subtitle should more properly be, "Risk Mitigation for Microsoft

Software." However, if you are using Windows, there is a good deal of

information in this book that, with some diligence and additional work on your part, can help improve your security.

Grimes starts off the book by listing some fallacies that we have always

believed. "You can't get a virus by simply reading an e-mail." (OK,

Microsoft has amply demonstrated that they've added virus capabilities to

their mail software.) "Malicious code can't harm hardware." (Well,

quibbles about terminology aside, it usually can't.) "A virus can't hide

from a booted write-protected diskette." (Ummm, I'm not sure that sentence

even \*means\* anything.)

Melissa and the Love Bug were serious nuisances, and even worse, but is it

really accurate to say that they shut down tens of thousands of networks?

This book is intended for intermediate and advanced users and system

administrators, and addresses only the Microsoft Windows operating systems.

While I would agree that Windows is the system most in need of virus

protection and help, this focus does limit the audience. Grimes

also tries to avoid the virus/worm/replicating trojan argument with the use of the term malicious mobile code, and states that the book does not deal with attacks and security holes, but the coverage of trojans, RATs (Remote Access/Administration Trojans/Tools), and browser attacks seems to contradict that position. (In fact, the more detailed description of "malicious mobile code," and the MMC acronym that Grimes creates, seems to be amply covered under the more commonly used term malware.)

Chapter one provides a very brief outline of some malware related concepts. Most of the chapter concentrates on the virus writing community, although only in a superficial way. Grimes obviously feels sympathetic towards virus writers, and presents their own stories without criticism or analysis. Some details of the MS-DOS operating system, as well as basic virus technologies, are given in chapter two. The programming particulars, and a bit of virus source code, are likely to be of more help to budding virus writers than to the defending sysadmins. There are copious errors in the information listed about specific viruses. Sometimes the material is careless, such as the assertion that Michelangelo formats hard drives (the original version overwrites sections of the disk, and only the disk booted from on the trigger date). In other places the wording is slipshod, such as the implication that a seldom seen screen artifact of the Jerusalem virus is somehow responsible for file deletion. (Oddly, while Grimes does not appear to have done serious research he has obviously read my stuff at

some point:

one of the examples is taken almost word for word from my writings. Other passages originating in my work are recognizable, although not quite as blatant.) The recovery advice is also suspect: he reiterates the rather dangerous suggestions to format the disk or use FDISK /MBR.

Some very useful information about Windows, particularly the 9x, NT, and higher versions, is presented in chapter three. The material does not often deal with malware as such, and, in a number of cases, details are either too particular or not specific enough. A few "native" Windows viruses are described in chapter four, along with some useful general security and recovery tips. Unfortunately, the virus detection and recovery tips are derivative, vague, and not always comprehensive. Chapter five has explanations of the VBA (Visual Basic for Applications) macro system in Microsoft Office applications, and lists some common macro viruses.

Chapter six lumps trojans, worms, backdoors, and DDoS (Distributed Denial of Service) packages together in a somewhat confusing manner. One useful inclusion in the material is a list of RAT utilized port numbers. The invention of real-time conferencing, or instant messaging, appears to be credited to AOL, in chapter seven, although various forms existed long before AOL's existence. All forms of chat or messaging seem to be lumped together in the chapter, although it concentrates on the technology and examples from IRC (Internet Relay Chat).

Chapter eight contains a reasonable overview of Web browser technologies, although Grimes makes the usual mistakes, such as confusing Secure HyperText Transfer Protocol (S-HTTP) with the https protocol specifier actually used by Secure Sockets Layer (SSL). A number of old program bugs and exploits are described in chapter nine. Most relate to browsers, although some depend on HTML enabled mail clients. The preventive measures listed, however, deal strictly with the settings on recent versions of Microsoft's Internet Explorer, and do not mention other browsers at all. Since Java applet bugs and exploits have been confined to implementation errors, it is difficult to understand why chapter ten was included in the book. Again, some older exploits are described, and there is a bit of confusion in the text between the applet sandbox model and the full Java security model. Chapter eleven examines the possibility of the malicious misuses of the ActiveX system, but first it spends a lot of time and space presenting the one security aspect of ActiveX: digital signatures. By doing so, Grimes is giving Microsoft way more than the benefit of the doubt. The text does, eventually, get around to pointing out some of the flaws in the Authenticode system, but the structure of the chapter works to downplay the dangers.

In chapter twelve, the Microsoft chauvinism that has been evident in prior sections ramps up to full throttle. Grimes states that it isn't just Outlook that can be exploited for e-mail viruses, any mail

client could be so abused. (He later has to tacitly admit that almost no other e-mail client has been so utilized, and none to the same extent.) There is even a paean of praise to Windows Script Host, the application that made the Love Bug possible. The material on virus hoaxes, in chapter thirteen, is a bit of a mix, but does have a good list of signs to watch for. Defence consists mainly of a generic security planning process and a reasonable, though brief, outline of the types of antiviral software, in chapter fourteen. Chapter fifteen finishes off with the usual look to the future.

Overall, the content is wide-ranging, but not complete. There is coverage of a broader range of topics than was the case with other recent books, such as Dunham (cf. BKBVRTPR.RVW) and Schmauder (cf. BKVRSPRF.RVW). However, depth of research and understanding of the problem is not in evidence. The material is very questionable in view of the number of errors Grimes makes in his retailing of details of specific viruses.

While some support and background content is included, the book is written in a very field independent style: at the end of the chapter you are simply supposed to do what Grimes tells you to, and believe what he says.

There is virus code in the book. Not extensively, perhaps, but it is there. Grimes justifies its presence by saying that it is not code for an entire virus, and that he has made changes to disable it in any case. Unfortunately, it is real code, for some important sections of viruses, and

the missing and changed bits aren't all that hard to spot. While it would not allow wannabe vxers to compile a complete virus right off the page, it would help any semi-competent code dweeb write a more functional virus. And, all protestations notwithstanding, it doesn't provide any help to the user or network manager.

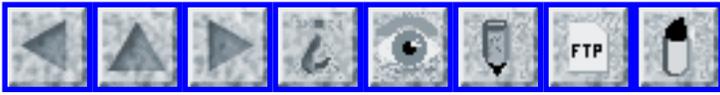
Aside from problems with the content, Grimes' organization and writing is careless and difficult to understand. The chapters address individual topics, and have a standard structure, but the structure is only a template. Within each topic the flow of sections and even paragraphs does not always course logically. The illustrations and figures are not very informative.

This is not a good book on viruses or malware. The breadth of coverage and detailed content on macro and e-mail virus technology does save it from being really awful: up to the summer of 2001 no other book has dealt with those topics in sufficient depth. And the MS-centrism does have one very positive advantage. If you absolutely must use Microsoft software and applications, the prevention sections of the various chapters do contain a lot of detail that will be useful in reducing the risk that you face.

copyright Robert M. Slade, 2001 BKMLMBCD.RVW 20010814  
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 21: Issue 73**

**Monday 5 November 2001**

## Contents

- [FAA Asleep at the Control Column?](#)  
[Bill Duncan](#)
- [Jilted boyfriend hacked into ex-girlfriend's Internet bank account](#)  
[PGN](#)
- [Kids' learning game site becomes porn site](#)  
[PGN](#)
- [Anonymous e-mailer convicted of cyberstalking](#)  
[Declan McCullagh](#)
- [Sony uses DMCA against Aibo Enthusiast's Site](#)  
[Monty Solomon](#)
- [RU-Blue? or RU-Yellow?](#)  
[PGN](#)
- [DeCSS is Speech](#)  
[James S. Tyre via David Farber](#)
- [Risks of concentrated power and the surveillance state](#)  
[Peter Wayner](#)
- [Risk of monoculture and exponential false AV positives](#)  
[Devon McCormick](#)
- [Fake ID anyone?](#)  
[Tim Rushing](#)

- [Bank assets disappear, convert customers into Euro-peons](#)  
[Paul van Dijken](#)
  - [DoS attack on Mac OS9](#)  
[Erann Gat](#)
  - [Conference management software reveals "hidden" authors](#)  
[Michael Ortega-Binderberger](#)
  - [Insecure promo from American Express](#)  
[Cameron Simpson](#)
  - [Re: ACT Election Electronic Voting](#)  
[Henry Grebler](#)
  - [Re: TD Bank Canada system crash](#)  
[Przemek Skoskiewicz](#)
  - [Re: Stray bomb caused by typo](#)  
[James R. Cottrell Jr.](#)
  - [Re: Int. Conf. on COTS-based Software Systems](#)  
[Kearton Rees](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

## ✶ FAA Asleep at the Control Column?

Bill Duncan <bduncan@beachnet.org>

Sun, 4 Nov 2001 17:15:16 -0500 (EST)

A few days ago while looking through the e-mail rejection logs, I was surprised to find some e-mail blocked by virtue of being in an RBL list and coming from a host in the FAA.GOV domain. The e-mail was obvious spam, as I'd blocked the same sender (from a domain in the UK) from various other addresses.

Being a new private pilot and with the recent of September events fresh in my mind, I quickly investigated. Sure enough, there was a host

on their  
network, loaded with software from that outfit in Redmond, and  
happily  
spewing relayed mail. (I tested whether it would relay mail  
from anywhere  
to anywhere else by telneting to its smtp port.)

Furthermore, to get on this exclusive RBL list, the e-mail relay  
must've  
been in operation for some time.

Imagining scenarios where relaying e-mail through the FAA system  
might at  
best be an embarrassment, and at worst might be some kind of a  
security  
threat, I immediately e-mailed whatever addresses I could find  
on their  
website as well as the usual postmaster@faa.gov etc. So far, no  
response,  
and according to my log files, I'm still rejecting spam from  
them.

While many US Federal Government agencies are discovering the  
virtues of  
Open Source for security, I'm dismayed to find that the FAA is  
still using  
software well known for insecurities on their website as well as  
other hosts  
connected to the Internet. Getting junk e-mail relayed through  
the FAA might  
be just an annoyance, but it might also point to other security  
issues  
there.

So if you get any e-mail from the FAA, be careful. It's  
probably just  
SPAM, but it might be worse.

Follow-up: Mon, 5 Nov 2001 15:41:11 -0500 (EST)

I didn't want to include the identifying IP address in the  
original  
submission, to protect the guilty, but it looks like they took

it off this morning. I tried pinging the address and they are no longer there. The last SPAM which was sent my way from that address was at 1:15 this morning EST.

Although I e-mailed about 4 addresses at the FAA, including one for emergency response, I've received no replies as yet. But I guess the message finally got through this morning. Maybe they'll take it as a wakeup call, which I didn't think they'd really need after the recent events...

Here's the last log entry from my mail log, with the local address changed. I'm using Exim.

```
2001-11-05 01:15:18 recipients from atos.faa.gov
[204.108.10.130] refused
2001-11-05 01:15:18 recipient <localname@domain.com> refused
  from atos.faa.gov [204.108.10.130]
  sender=<masterdisc8745@gmx.co.uk> (host_reject_recipients)
```

Bill Duncan, VE3IED <http://www.beachnet.org> bduncan@BeachNet.org  
+1 416 693-5960

---

## **✶ Jilted boyfriend hacked into ex-girlfriend's Internet bank account**

"Peter G. Neumann" <neumann@csl.sri.com>  
*Wed, 31 Oct 2001 9:37:30 PST*

After their relationship ended, Cheug Wing-hang took 420 pounds (HK?) from his girlfriend's HSBC Internet bank account. He was convicted on four

counts of theft and five counts of dishonest computer access.  
The \*South  
China Morning Post\* reported he will be sentenced on 13 Nov 2001.  
[[http://www.ananova.com/news/story/sm\\_431974.html](http://www.ananova.com/news/story/sm_431974.html)]

[Despite the lack of specificity on what kind of pounds were  
involved,  
we can assume that his girlfriend did not weigh more than 500  
pounds.]

---

## ⚡ Kids' learning game site becomes porn site

"Peter G. Neumann" <neumann@csl.sri.com>  
*Wed, 31 Oct 2001 10:10:48 PST*

The Web sites at moneyopolis.org and moneyopolis.com once housed  
an online  
interactive children's game created by Ernst & Young to help  
youngsters in  
grades 6 to 8 learn about finances. Recently, E&Y gave up the .  
org domain,  
which has now become Euro Teen Sluts (TM), registered in  
Yerevan, Armenia.  
Old bookmarks beware. [Source: The Washington Post, 25 Oct  
2001; PGN-ed]

[I presume that this issue of RISKS will succumb to some  
filtering  
because of its mentioning the name of the new owner of the  
domain.]

---

## ⚡ Anonymous e-mailer convicted of cyberstalking

Declan McCullagh <declan@well.com>  
*Wed, 31 Oct 2001 08:39:46 -0800 (PST)*

A California man who used a public library computer terminal to send anonymous e-mail threats to a Michigan man has been convicted by a jury of cyberstalking. The prosecution used circumstantial evidence to prove its case, since no logs of the e-mails or computer users were kept by the library. <http://www.siliconvalley.com/docs/news/depth/stalk103101.htm>

---

## **✦ Sony uses DMCA against Aibo Enthusiast's Site**

Monty Solomon <monty@roscom.com>

*Thu, 1 Nov 2001 20:39:12 -0500*

Sony Dogs Aibo Enthusiast's Site

Courts: The company uses a controversial law to stop owners from altering the robotic pet. Some consumers balk.

Sony Corp. is using a controversial U.S. law aimed at protecting intellectual property to pull the plug on a Web site that helps owners of Aibo, Sony's popular and pricey robotic pet, teach their electronic dogs new tricks. Aibo owners are outraged, and hundreds have vowed to stop buying Sony products altogether until the company backs off. Sony has sold more than 100,000 Aibos worldwide since 1999, at prices ranging from \$800 to \$3,000. The dogs have spawned a community of enthusiasts who fuss over the mechanical marvels as if they were real canines. [Source:

Article by Dave

Wilson and Alex Pham, \*Los Angeles Times\*, 1 Nov 2001]

<http://www.latimes.com/business/la-000086726nov01.story?coll=la-headlines>

---

## ✶RU-Blue? or RU-Yellow?

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

*Thu, 1 Nov 2001 19:59:47 PST*

The United States is changing the color of food ration packets it is dropping in Afghanistan because they are the same color -- yellow -- as unexploded cluster bombs. Gen. Richard Myers, chairman of the Joint Chiefs of Staff, said the United States will change the color of the food packets to blue. [Thanks to Mike Hogsett, from <http://www.cnn.com/2001/US/11/01/gen.attack.on.terror/index.html>]

[Now, you will get very "blue" if you choose the yellow, and you will be "yellow" if you do not choose the blue. Watch out for the Yellow Submarine Sandwich. PGN]

---

## ✶DeCSS is Speech (James S. Tyre, from IP)

David Farber <dave@farber.net>

*Thu, 01 Nov 2001 19:07:37 -0500*

[Summary: Source code is speech. Object code is not speech. PGN]

>Date: Thu, 01 Nov 2001 13:02:54 -0800  
>From: "James S. Tyre" <jstyre@jstyre.com>  
>Subject: DeCSS is Speech

>> "Like the CSS decryption software, DeCSS is a writing  
composed of computer  
>> source code which describes an alternative method of  
decrypting  
>> CSS-encrypted DVDs. Regardless of who authored the program,  
DeCSS is a  
>> written expression of the author's ideas and information  
about decryption  
>> of DVDs without CSS. If the source code were "compiled" to  
create object  
>> code, we would agree that the resulting composition of zeroes  
and ones  
>> would not convey ideas. (See generally *Junger v. Daley*,  
*supra*, 209 F.3d  
>> at pp. 482-483.) That the source code is capable of such  
compilation,  
>> however, does not destroy the expressive nature of the source  
code  
>> itself. Thus, we conclude that the trial court's preliminary  
injunction  
>> barring Bunner from disclosing DeCSS can fairly be  
characterized as a  
>> prohibition of "pure" speech."

> This is *\*not\** from the Second Circuit, where we did the amicus  
brief.

> This is from the California state court trade secrets case,  
DVDCCA

> v. Bunner, in which the court today reversed the preliminary  
injunction

> issued against the Defendants. PDF Opinion:

> <http://www.courtinfo.ca.gov/opinions/documents/H021153.PDF>

> James S. Tyre  
jstyre@jstyre.com

mailto:

> Law Offices of James S. Tyre  
(fax)

310-839-4114/310-839-4602

> 10736 Jefferson Blvd., #512

Culver City, CA

90230-4969

> Co-founder, The Censorware Project

<http://>

[censorware.net](http://censorware.net)

For IP archives see:

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

---

## **✶ Risks of concentrated power and the surveillance state**

Peter Wayner <[pcw@flyzone.com](mailto:pcw@flyzone.com)>

*Fri, 26 Oct 2001 08:45:55 -0400*

Federal prosecutors said Mr. Hanhardt used law enforcement computers and other databases to get information on traveling jewelry sales representatives, including itineraries and car rental information.

Prosecutors said many of the thefts were from the rented automobiles.

[Source: <http://www.nytimes.com/2001/10/26/national/26THEF.html>,

\*The New York Times\*, 26 Oct 2001]

Mr. Hanhardt was Chief of Detectives for the Chicago Police Department. His gang, which operated from the early 1980's to 1998, reportedly stole more than \$5 million. This may not be the best estimate because as part of his plea bargain, he's going to pay \$4.8 million and cash equal to half of the equity in his home. There were 6 people in the gang. We probably don't know the full extent of his crime spree.

---

## ✶ Risk of monoculture and exponential false AV positives

Devon McCormick <devonmcc@yahoo.com>

Sat, 27 Oct 2001 09:04:53 -0700 (PDT)

I'd like to point out two related risks: the risk of monoculture and the risk of a potential exponential increase in spurious collisions between legitimate software and anti-virus.

First, I'll summarize a complaint (on a mailing list) from a consultant: a popular AV (anti-virus) software package may be disallowing operation of normal software as being possibly viral. Of course, the "safe" solution The AV chooses is to disallow some file access by the offending software.

This simplistic, inflexible default is exacerbated by similar inflexibility on the part of the IT group which tends toward monoculture, admittedly in the face of overwhelming complexity. By monoculture, I mean restricted support of or interest in any software outside a narrow list of approved vendors.

The consultant uses a niche product with which the IT department is unfamiliar, therefore they lack the competence to check out his claim of innocence so he must assume the burden of proof. Furthermore, he has no authority to conduct a simple test, switching the anti-virus off and on again to show that it, not his software, is the problem.

The risk of monoculture is further raised by the speculation that the the AV

conflict may be caused by his software directly writing files with binary data instead of using a more standard, and increasingly more common, access method such as ODBC.

This leads us to the 2nd risk: (possibly) exponentially increasing AV false positives.

I once had a similar problem with an AV: an optimization I was running triggered a virus warning and stopped the run. I suspected that the bit pattern of an intermediate file was matching that of a "known virus", so I shortened the inputs to the optimization by the least significant digit, thus slightly changing these intermediate values, and it ran without a problem after that. Fortunately I knew my results were not sensitive to such a small change.

As in the case above, I was using specialized, niche, software. However, the other risk this illustrates is the realization that the number of false positives from AV is the product of 2 numbers: how many different signatures (indicators of known viruses) being checked and the number of different intermediate results any software may produce.

Both of these factors are increasing over time. This increase may be exponential (in the loose sense) because, at first glance, this likelihood of collision resembles the Birthday Problem. This is the well-known, non-intuitive result that there's about a 50% chance that 2 people, out of a random group of 25 or 26, will share a common birthday.

Similarly, the chance of a spurious AV hit depends on the product of the linear increase of the 2 factors mentioned.

---

## **⚡ Fake ID anyone?**

Tim Rushing <tim@rushing.com>

*Thu, 25 Oct 2001 09:55:14 -0500*

I live in Indiana and recently lost my wallet on a weekend. I was pleasantly surprised that the bank allowed me to cash a check without id or check card by punching my ATM code into the keypad at the teller's window. However, the process for actually getting my license replaced at the state license bureau was not as inspiring.

Initially, I was impressed. I had gone with an expired passport (picture taken in 1986 when I was much younger and lighter), bank statement and a number of other items. When I arrived, they compared my proofs of identity against a checklist. Apparently, various items are worth between 1 and 6 points, with a valid driver's license worth 6 points and my bank statement worth 1. You need 6 points to get a driver's license issued to you. With the passport, I had 7 points. Unfortunately, the passport was only worth 3 if it was less than 2 years expired.

So, armed with the list, I made another trip home and easily returned with 8 valid points. I made it past the screener to get to the person at the

terminal who actually sets up the license. She also carefully checked through all my documentation, handed it back to me, turned to her computer and asked, "Name?" She even had my spell my last name. No attempt to correlate the name with the documentation and she had written nothing down from my paperwork. Now, Indiana does have digital pictures on the license, so it is possible that once she pulled it up, she had a picture of me to look at. I wasn't reassured.

Once again, a great demonstration that a well-designed security system can be easily undermined in implementation.

Tim Rushing

[And airlines are contemplating using smart cards for fast access by passengers! PGN]

---

## ✶ Bank assets disappear, convert customers into Euro-peons

"Paul van Dijken" <tapvd@xs4all.nl>

*Wed, 31 Oct 2001 22:49:12 +0100*

On 29 Oct 2001, my sister and brother-in-law experienced one of their worst nights ever. When trying to pay some bills using the Internet site of the SNS bank (one of the major banks in the Netherlands), the transactions were rejected, because no sufficient amount was available. This was strange, because normally a couple of thousand guilders (a few thousand

dollar, about half) should be there. When he checked his savings, the entire amount was gone. All accounts had a zero amount.

Thinking on how they should pay the new shoes for the children, etc., they lay awake all night. The next morning, my brother-in-law arrived at work in a terrible temper. When asked, he explained to his colleagues the entire story and tried to show it. To his relief, all amounts were back, but this time in euros. Apparently the bank had gone through the euro conversion that night, but failed to shutdown its website or to warn its customers.

Fortunately, my brother-in-law has a strong heart.

[Good thing. He needed a Eurologist, not a Cardiologist. PGN]

---

## ⚡ DoS attack on Mac OS9

Erann Gat <gat@flownet.com>

*Mon, 5 Nov 2001 11:51:53 -0800 (PST)*

This is an old RISK, but I haven't seen it mentioned here before. Macintosh OS9 comes with a "multiple user" control panel that provide password protection. Trouble is, to change a password you don't have to type in the old password again, and you don't have to confirm the new password. So a malicious user who gains physical access to the machine can render that machine useless by changing the password and shutting the machine down. You

get the same result from a typo too. If what you actually typed as your new password isn't what you think you typed you're hosed. Poor Apple. They must be finding it hard to get good help these days.

Erann Gat <gat@flownet.com>

---

## ✂ Conference management software reveals "hidden" authors

Michael Ortega-Binderberger <miki@ics.uci.edu>

*Fri, 26 Oct 2001 00:56:30 -0700 (PDT)*

Conference paper submissions are hardly a life and death issue, but I just found a problem when submitting a paper.

The ACM SIGMOD conference is in its second year of a new double blind reviewing policy to improve fairness. You register a paper, write the names of the authors in a form, but not in the actual pdf submission, which only carries the paper id. In this environment, the idea of keeping authors hidden is of some value. While registering a paper, the Microsoft conference management software <http://cmt.research.microsoft.com/cmt/> told me one of my co-authors was already registered in the system, and whether I truly wanted to add him to my paper. This was my advisor, and as it turns out, another student is also submitting a paper, which is fine. But in general I could register any bogus paper, and give names of "competitors" and find who else is up to submitting papers to the conference.

An interesting vulnerability given the stated aims of double blind reviewing.

Michael Ortega-Binderberger, CS U.Illinois Urbana, on loan to U. C. Irvine  
miki@acm.org, miki@ics.uci.edu, miki@computer.org, m.ortega@ieee.org

---

## ***✶* Insecure promo from American Express**

Cameron Simpson <cs@zip.com.au>  
*Mon, 5 Nov 2001 21:57:39 +0000*

Today I received an an e-mail from AmEx promoting its Online Services, with offers of a chance to win lots of reward points if I sign up. However, there are enough bogus things in this missive to make me want to check very thoroughly that this actually comes from AmEx.

The first, and minor, point is the From: address:  
dtwnonenrollees+671692.836250193.4@1.americanexpress.com.au  
[Numbers mangled for privacy reasons.]

Looks pretty bogus, eh? I suspect that it's a bounce detector from the shape of it. [Checks... the MXs are bounce.exactis.com. and reply.exactis.com. which are pretty suggestive.] There's even a note at the bottom of the message saying "Please do not reply to this e-mail for any enquiries - messages sent to this address cannot be answered." It's only a list removal address, with apparently a 3 week(!) implementation time.

The second, and major, point is the contact URL. Look at this:

<http://tm0.com/AmericanExpress/sbct.cgi?s=.....>  
[I've stripped off the identifying parameters.]

There's no sign whatsoever that this is a bona fide AmEx host! A whois on tm0.com says nothing useful either:

Domain Name: TM0.COM  
Registrar: NETWORK SOLUTIONS, INC.  
Whois Server: whois.networksolutions.com  
Referral URL: <http://www.networksolutions.com>  
Name Server: NS01.LODO.EXACTIS.COM  
Name Server: NS00.LODO.EXACTIS.COM  
Updated Date: 27-oct-2001

Internic.net doesn't give an answer at all. So this would easily be a bogus domain by someone harvesting credit card information. Now, I happen to have a tool for this kind of thing and it says:

```
GET http://tm0.com/AmericanExpress/sbct.cgi?s=.....
REDIRECT(302) to http://www.americanexpress.com.au/onlineservices
GET http://www.americanexpress.com.au/onlineservices
REDIRECT(302) to http://home3.americanexpress.com/australia/onlineservices
GET http://home3.americanexpress.com/australia/onlineservices
REDIRECT(302) to http://home3.americanexpress.com/australia/onlineservices/
GET http://home3.americanexpress.com/australia/onlineservices/
REDIRECT(302) to https://www48.americanexpress.com/iestm/eoi/jsp/en_AU/logon/LogLogon.jsp?Face=en_AU&DestPage=https%3A%2F%2Fwww48.americanexpress.com%2Fen%2Fintl%3Frequest_type%3Dintl_CardsListHandler%26Face%3Den_AU
```

and off into https land it goes. So this URL does hand off to

Amex (with great inefficiency), and so the necessary degree of subversion is somewhat greater, requiring some DNS hacking. Or at least it does if my query tool goes there (in my paranoid musings I can imagine the tw0.com server only behaving suspiciously if the User-Agent matches one of the popular browsers, which my tool does not.) But how is the average user to check this? They can't. I expect I should be thankful (I'm merely surprised) that this was a plain text message; if it were HTML then recipients would have even less hint about the suspect URLs.

What else to fear? The opening URL is plain HTTP, liberally adorned with presumably identifying numbers. Somewhat insecure also.

If done properly, this should have been a direct HTTPS like to an obviously AmEx owned domain. There are no contact details on the e-mail except these URLs. I call AmEx customer service and the first thing they want is my card number. I'm now sufficiently soured on the whole thing that I just put the phone back down:-)

The RISK? Aside from the chance this actually is a scam (which I doubt, but only after digging around a bit), this is exactly the kind of message the naive user should never respond to. Yet such practices, like M\$'s loathsome practice of publishing documents as .exe files, actively encourages such laxness and complete faith in third parties. Yea, even in \*unknown\* third parties as in this case!

This does nothing for my confidence in them, and is somewhat

ironic while  
they're actively promoting their "blue" smartcard enhanced  
credit card,  
which somehow offers improved fraud security (in totally  
nebulous terms  
as near as I can tell so far).

Cameron Simpson, DoD#743  
[com.au/~cs/](http://www.zip.com.au/~cs/)

cs@zip.com.au

<http://www.zip.com.au/~cs/>

---

## ✦ Re: ACT Election Electronic Voting (Polette, [RISKS-21.72](#))

Henry Grebler <henryg@optimation.com.au>

Wed, 31 Oct 2001 09:57:44 +1100

> The 11,340 pre-poll electronic votes were supposed to have  
been counted just  
> after the polls closed at 6pm AEST but took about 90  
minutes ...

Give me a break! These numbers just don't add up. "11,340 pre-  
poll  
electronic votes" would not strain the resources of my \$2  
calculator.

"discs for the eight polling stations" - in other words, 8  
floppy disks -  
took 90 minutes to load ... because the entire population of  
Australia who  
actually cared enough to access the website - that's all 10 of  
us - resulted  
in them "getting lots of hits on our internet site".

They may well have had problems, but the evidence presented does  
not support  
the conclusions.

Finally, paying attention to the so-called problem of getting  
delayed

results runs the RISK of not addressing all the real security RISKS mentioned in previous editions of RISKS.

---

## ✉ **Re: TD Bank Canada system crash (Akerman, [RISKS-21.72](#))**

"Przemek Skoskiewicz" <przemek@synchronicity.com>

*Mon, 5 Nov 2001 17:11:00 -0500*

> The bank's computer systems have all sorts of "redundancies" built in ...

and the very next entry from PGN describes "ANOTHER SRI-wide Power Outage"

due to the pressing of an incorrect button!

Sometimes I feel that RISKS readers expect to live in a perfect world. A remarkable thing about the Toronto-Dominion bank failure would be if it had accepted the transactions and lost them, or erased customer data, rather than it being down for the weekend. Do we really expect to spend so much time and money designing our systems against *every* conceivable occurrence? Besides an inconvenience, was the bank's downtime really such a dramatic event that it ought to have designed against random board failures?

And what about the SRI's power failure? I'm sure that SRI's power backup systems are some of the best thought-through and designed systems in place, yet one press of the wrong button took them down. Does this mean that their design was an utter failure and they should start from scratch?

I think that sometimes we are better off accepting such "random" occurrences, not bothering too much about them and treating them as normal annoyances of modern life. Like whenever I walk out of my apartment and there are 3 empty taxis lined up in front, but whenever I actually need one, there isn't one for miles, :-)

Przemek Skoskiewicz

---

**⚡ Re: Stray bomb caused by typo (Jacobson, [RISKS-21.71](#))**

"James R. Cottrell Jr." <jxc@mitre.org>

*Mon, 05 Nov 2001 14:10:45 -0500*

I believe the submitter missed the point of the original submission. If the check digit is calculated such that transposition of two legal values (latitude 89.0 and 80.9) provides a different value, then it doesn't matter that all possible latitudes are valid. I believe this was done with bank account numbers in the 1970s to reduce/eliminate typos.

Jim Cottrell      jxc@mitre.org    1-781-271-6475

---

**⚡ Re: Int. Conf. on COTS-based Software Systems ([RISKS-21.70](#))**

Kearon Rees <Kearon.Rees@bt.com>

*Thu, 25 Oct 2001 14:26:57 +0100*

In Europe the UK-based Safety-Critical Systems Club (<http://www.safety-club.org.uk/>) has also been looking at the issues raised by the use of COTS, in this case for use in safety-critical systems - April 2001 (<http://www.safety-club.org.uk/advert/CaS.html#Slides>).

Kearton Rees, BTextact Technologies, Adastral Park, Martlesham, Ipswich IP5 3RE, UK [Kearton.Rees@bt.com](mailto:Kearton.Rees@bt.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 21: Issue 74

**Sunday 11 November 2001**

## Contents

- [Programming error scrambles election results](#)  
[Geoff Kuenning](#)
- [Yet another Internet voting risk](#)  
[Rebecca Mercuri](#)
- [Election problems before the election in Virginia](#)  
[Jeremy Epstein](#)
- [Possible radiation therapy risk](#)  
[Herbert Kanner](#)
- [Risks of belief in identities](#)  
[PGN](#)
- [Stealing MS Passport's Wallet](#)  
[Mike Hogsett](#)
- [Security hole in cash machines](#)  
[Andrew Brydon](#)
- [UK: liberties fears over mobile-phone details](#)  
[Monty Solomon](#)
- [Dutch police 'bombard' stolen cell phones with SMS](#)  
[Monty Solomon](#)
- [Australian computer hacker jailed for two years](#)  
[Peter Deighan](#)

- [Even professional organizations forget about certificate expiration](#)  
[Jeremy Epstein](#)
  - [Children's medical records released on the Web](#)  
[Conrad Heiney](#)
  - [Glitch in iTunes Deletes Drives](#)  
[Monty Solomon](#)
  - [Dates in Visual Basic](#)  
[John Sullivan](#)
  - [Excel and non-decimal dots](#)  
[magical via Mark Brader](#)
  - [Sweden's public radio reportedly bans SETI from office computers](#)  
[Ulf Hedlund via Declan McCullagh](#)
  - [Random failures](#)  
[Andrew Brydon](#)
  - [Re: Another SRI-wide Power Outage](#)  
[Marcus L. Rowland](#)
  - [Re: Kids' learning game site becomes porn site](#)  
[Daniel P. B. Smith](#)  
[Ian Young](#)  
[Paul Bowers](#)
  - [Re: DeCSS is Speech](#)  
[Amos Shapir](#)
  - [Re: DoS attack on Mac OS9](#)  
[William Kucharski](#)  
[Carl Maniscalco](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

## ✶ Programming error scrambles election results

Geoff Kuenning <geoff@cs.hmc.edu>

Sat, 10 Nov 2001 14:16:27 -0800

A San Bernardino County election last Tuesday was counted incorrectly due to a programming error. According to the *\*Los Angeles Times\**, a

veteran county  
employee claimed to have tested his code, but apparently had not  
actually  
done so. Some ballots were counted starting at the middle  
(sounds like an  
uninitialized loop variable); others were counted "from the  
bottom up"  
(don't ask me how). The unnamed employee has been suspended from  
programming duties. A consulting firm has now been brought in  
to verify the  
software for this and all future elections, something that  
should have been  
standard practice all along.

In some races, heavily favored incumbents "lost" to unknowns who  
hadn't  
campaigned at all. The error was uncovered when officials  
noticed that the  
count for one race showed no votes counted.

Especially telling is the following paragraph in one the Times  
stories:

"County officials said the good news is that using a card-  
counting system  
means that ballots are still around to be recounted. If the  
same error  
had occurred with an electronic voting system, there would be  
no paper  
record, West said."

We've been telling them for years. But I doubt they'll learn  
their lesson.

Geoff Kuenning    geoff@cs.hmc.edu    <http://www.cs.hmc.edu/~geoff/>

[The results of 33 races were seriously in doubt, and all  
85,000 ballots  
for 82 races will be recounted. Also noted by Erann Gat. PGN]

## **✶ Yet another Internet voting risk**

Rebecca Mercuri <Mercuri@acm.org>

*Tue, 6 Nov 2001 14:50:56 -0500 (EST)*

I was working at the polls in Mercer County NJ during the 6 Nov 2001 election and heard from a number of people whose spouses and/or children had applied for absentee ballots (since they would not be able to vote at the polls) but did not receive them. Mercer County is in the midst of the Anthrax mailing zone, with 3 post offices affected. Apparently, in some of the cases, the application for the absentee ballot was not received in time, and in other cases the absentee ballots were not received by the voters in time.

How this relates to Internet balloting -- most schemes, including the one outlined by the California Task Force, would require the validation process and issuance of the Internet voting password to be issued by postal mail. A mail hold-up such as the one we are experiencing in New Jersey could adversely affect the process.

In short, the best way to validate voters is in person.

---

## **✶ Election problems before the election in Virginia**

Jeremy Epstein <jepstein@webmethods.com>

*Wed, 31 Oct 2001 09:05:50 -0500*

Like almost all U.S. states (\*), Virginia is undergoing redistricting as a result of the 2000 census. As a result, some people got new polling places.

According to

<http://www.washingtonpost.com/wp-dyn/articles/A14523-2001Oct30.html>

Fairfax County sent electronic updates to the state for inclusion in the state's database to reflect local redistricting, and the state sent a new master database back, which lost about 18,000 of the updates. Unfortunately, Fairfax County used the erroneous data to send out voter information, and had to send out a second set of instructions.

There's the predictable finger-pointing as to who's at fault for the snafu.

All goes to prove that there are plenty of computer-related risks in elections, and that's before you even get to the polling place!

(\*) There may be some states where there's no redistricting. For example, Wyoming only has one representative, so there's no need for statewide redistricting, although there may be local redistricting.

---

## **✶ Possible radiation therapy risk**

Herbert Kanner <kanner@acm.org>

*Sat, 10 Nov 2001 11:59:32 -0800*

As a patient being irradiated by a Varian linear accelerator, it interested me to be told by a technician that when they are behind schedule

it is usually because of a computer crash. He said that the accelerator is controlled by "three computers that talk to each other." I inquired further and found out that they are PCs running Windows 2000. Not exactly confidence inspiring!

Herbert Kanner <kanner@acm.org> 650-326-8204

---

## ✶ Risks of belief in identities

"Peter G. Neumann" <neumann@csl.sri.com>  
*Sat, 10 Nov 2001 11:54:17 PST*

For those of you who might believe that national ID cards might be a good idea, check out the December 2001 \*Commun.ACM\* Inside Risks column by me and Lauren Weinstein, previewed on my Web site <http://www.csl.sri.com/neumann/insiderisks.html> in anticipation of a U.S. House hearing next Friday on that subject.

It is not just the cards themselves that would entail risks, but even moreso all of the supporting infrastructures, widespread accessibility to networking, monitoring, cross-linked databases, data mining, etc., and particularly the risks of untrustworthy insiders issuing bogus identification cards -- as happened a few years back on a large scale in the Virginia state motor vehicle agency ([RISKS-11.41](#)).

The latest item on the ease of getting phony or illegal or unchecked

identification papers is found an article by Michelle Malkin (Creators Syndicate Inc.), which I saw in the \*San Francisco Chronicle\* on 10 Nov 2001: Abdulla Noman, employed by the U.S. Department of Commerce, issued bogus visas in Jeddah, Saudi Arabia, in one case in 1998 charging approximately \$3,178. The article also notes a variety of sleazy schemes for obtaining visas, in some cases without ever appearing in person and without any background checks, and in other cases for ``investments'' of a hundred and fifty thousand dollars. The article concludes with this sentence: ``Until our embassy officials stop selling American visas blindly to every foreign investor waving cash, homeland security is a pipe dream.''

I'm not sure that conclusion is representative of the full nature of the problem of bogus identification, but the problem is clearly significant.

A driver's license or a passport or a visa or a National ID card is not really proof of identity or genuineness or anything else.

---

## ✶ Stealing MS Passport's Wallet

Mike Hogsett <hogsett@csl.sri.com>

*Fri, 02 Nov 2001 14:51:52 -0800*

From : <http://www.wired.com/news/technology/0,1282,48105,00.html>

By cobbling together a handful of browser-based bugs with flaws in Passport's authentication system, Slemko developed a technique to

steal a person's Microsoft Passport, credit card numbers -- and all, simply by getting the victim to open a Hotmail message.

---

## **Security hole in cash machines**

Andrew Brydon <andrew@isbjorn.demon.co.uk>

*Fri, 9 Nov 2001 05:53:32 +0000*

[http://news.bbc.co.uk/1/hi/english/sci/tech/newsid\\_1645000/1645552.stm](http://news.bbc.co.uk/1/hi/english/sci/tech/newsid_1645000/1645552.stm)

By BBC News Online technology correspondent Mark Ward

A serious weakness has been discovered in the methods used by banks to protect the number that lets you get money from a cash machine. Researchers from the University of Cambridge have found that the computer systems which check that these numbers are valid are easy to defeat. They warn that unscrupulous insiders could exploit these weaknesses to raid customer accounts. The researchers have called on banks to revise their security arrangements and use more open procedures to protect customers' cash.

... The physical construction of the cryptoprocessors is certified to a high standard to ensure that the boxes cannot be forced to give up the keys they use to scramble data. Any physical tampering with the box makes them destroy the keys they use. [However,] security researchers Michael Bond and Richard Clayton have found serious weaknesses in the software cryptoprocessors use to handle the encryption keys as they talk

to different  
programs. ... using the clues provided by the leaky software,  
the cracking  
time can be reduced to just 24 hours.

Andrew Brydon, Systems & Software Safety Analyst, Lancashire, UK

---

## **UK: liberties fears over mobile-phone details**

Monty Solomon <monty@roscom.com>

*Tue, 30 Oct 2001 21:02:14 -0500*

Records which map out users' whereabouts held indefinitely  
Stuart Millar and Paul Kelso, *\*The Guardian\**, 27 Oct 2001

One of the fastest growing mobile phone providers is  
indefinitely storing  
information that allows its customers' movements over the last  
two years to  
be mapped to within a few hundred metres. As the government  
rushes through  
emergency anti-terror legislation that would require vast  
amounts of  
electronic communications data to be retained in the name of  
national  
security, *\*The Guardian\** has established that Virgin Mobile has  
been storing  
the location records of its 1 million customers since the  
network launched  
in November 1999. Last night, the privacy watchdog, the  
information  
commissioner, told the Guardian that it would be investigating  
the practice  
to establish whether it contravenes regulations governing  
retention of  
communications data. [...]

<http://www.guardian.co.uk/mobile/article/0,2763,581763,00.html>

---

## **⚡ Dutch police 'bombard' stolen cell phones with SMS**

Monty Solomon <monty@roscom.com>

*Tue, 6 Nov 2001 10:03:47 -0500*

Dutch Police 'Bombard' Stolen Cell Phones With SMS  
By Andrew Rosenbaum, Special to Newsbytes, AMSTERDAM,  
NETHERLANDS, 05 Nov 2001

The Amsterdam police have been using short messaging system (SMS) missives to block the use of stolen cell phones, and while the campaign has been successful, mobile providers are concerned about the cost and bandwidth strain of the campaign.

About four months ago, the Amsterdam police began cooperating with the national telecommunications provider, KPN Telekom. When stolen phones are reported, the police asked KPN to use the phone to locate the telephone number. Then, every three to five minutes, the police sent SMS messages to the telephone saying, "Warning, this is a stolen telephone, using it is against the law -- stealing it is a felony." ...

<http://www.newsbytes.com/news/01/171836.html>

---

## **⚡ Australian computer hacker jailed for two years**

Peter Deighan <deighanp@ozemail.com.au>

*Wed, 31 Oct 2001 20:03:45 +1100*

This from Australian Broadcasting Corporation web site, 31 Oct 2001

URL = <http://www.abc.net.au/news/newslink/nat/newsnat-31oct2001-96.htm>

Vitek Boden, a computer hacker who hacked into the sewage control computer and intentionally released caused thousands of litres of raw sewage into creeks and parks on the lower Queensland Coast (and the grounds of the local Hyatt Regency), has been jailed for two years by a Maroochydore District Court jury. [PGN-ed]

An unexpected Risk? Wonder what the design decision was: perhaps to save on call-back costs for control staff?

[also noted by Derek Ross and George Michaelson. PGN]

---

## **✶ Even professional organizations forget about certificate expiration**

Jeremy Epstein <jepstein@webmethods.com>

*Mon, 5 Nov 2001 09:23:29 -0500*

If you visit <https://swww2.ieee.org/> (the site used for on-line renewal of IEEE membership), you'll learn that the certificate expired on Oct 31st 2001. I reported this on Nov 1st to IEEE, and as of today (Nov 5th), it hasn't been fixed.

I'm curious how many other people noticed/reported it, or if everyone just clicked through due to the vast quantity of similar problems on the Internet. What good is certificate expiration if it gets ignored by users?

---

## ✶ Children's medical records released on the Web

Conrad Heiney <conrad@fringehead.org>

*Wed, 7 Nov 2001 10:45:58 -0800*

The University of Montana released confidential psychological records of children on the World Wide Web, according to the \*Los Angeles Times\*:

<http://www.latimes.com/news/nationworld/nation/la-110701private.story>

Four hundred pages of documents about at least 62 children were posted, including in some cases complete name and address information along with results of psychological testing. According to the times, the data was available for eight days starting October 29 and included confidential and detailed summaries of patients' psychiatric conditions in much more detail than in previous similar accidental releases of information. The University indicated that errors by students or technical employees were likely to be at fault.

The obvious Risk of electronic medical records is once again proved in an especially painful way.

Conrad Heiney conrad@fringehead.org <http://fringehead.org>

---

## **✶ Glitch in iTunes Deletes Drives**

Monty Solomon <monty@roscom.com>

*Tue, 6 Nov 2001 09:58:07 -0500*

Glitch in iTunes Deletes Drives, By Farhad Manjoo, 5 Nov 2001

Some Macintosh users who rushed to download the latest version of iTunes -- Apple's popular digital-music player -- were singing a song of woe on Friday. A bug in the installation procedure caused the application to completely delete their computers' hard drives. Apple issued an alert and a fixed version of iTunes 2 on Saturday morning, and the company urged people to remain calm. [...]

According to Mac experts who examined the code of the buggy iTunes installer, the problem arose from a very tiny programming mistake -- a forgotten quote mark.

Instead of typing the line "\$2Applications/iTunes.app", a bleary-eyed coder had instead typed the disastrous \$2Applications/iTunes.app, according to a message on MacSlash. [...]

<http://www.wired.com/news/technology/0,1282,48149,00.html>

---

## Dates in Visual Basic

John Sullivan <john.sullivan@thermoteknix.co.uk>

*Fri, 9 Nov 2001 16:56:45 +0000*

I was just writing a test-harness in Visual Basic (VB6 SP5) when I noticed the following annoying and potentially downright dangerous behaviour.

Part of the code generated a series of dates, and I'd entered the start date as a literal date of the form #2001-11-08#. This worked fine as I expected and as it wasn't at all important at this stage so I didn't look twice at what I'd just typed.

When I came back to it today, I noticed it read #11/8/2001#. Now, I never code dates in non-ISO format if possible, and being in the UK with my locale set to UK never, ever, use US mm/dd format unless I know it's the only format a broken program accepts. Retyping it showed that the date was changed in front of my eyes:

```
#2001-11-08# becomes #11/8/2001# (2001-11-08)
#11/8/2001#  becomes #11/8/2001# (2001-11-08)
#8/11/2001#  becomes #8/11/2001# (2001-08-11)
#15/11/2001# becomes #11/15/2001# (2001-11-15)
```

It changes as soon as the cursor left the line. So you type it, check it, find it correct, go off somewhere else, blam!

The first has reduced the comprehensibility of the code. The second and third give no feedback that they're not conforming to the current locale.

The last two show that VB is not even being consistent in its

parsing.

The Risks:

Dumb programs thinking they're smart enough to change a programmer's code can lead to unpredictable behaviour. If you assume that what you type is what gets saved then you may not even notice, and errors in strings of numbers are immediately less obvious than structural or logical errors.

If I (or a colleague) came back to the first example in a few months time, will we know whether it means 8th Nov or 11th Aug? It would be natural to assume it's using the current locale, but in this case it isn't. What I actually typed was unambiguous.

I use VB, and dates in VB, so rarely that I may not even remember this behaviour myself a year or two down the line. Thankfully I don't have to use this noddy little toy for writing Real Programs in.

---

## **✶ Excel and non-decimal dots**

Mark Brader <msb@vex.net>

*Wed, 7 Nov 2001 13:43:25 -0500 (EST)*

\* From: magical@rahul.net  
\* Newsgroups: alt.usage.english  
\* Subject: Re: Telephone Area Code  
\* Message-ID: <7bqiutgjjqqgltu29qd6ak615c14pbcfavo@4ax.com>  
\* Date: Wed, 07 Nov 2001 17:07:08 GMT

On Wed, 07 Nov 2001 07:54:15 GMT, in alt.usage.english, David Hecht <davidhecht@prodigy.net> created

> The US convention (AAA)BBB-CCCC is not just evolving into AAA-BBB-CCCC;  
> now I'm seeing more and more of the "international" style: AAA.BBB.CCCC  
> . This appears in some "chic" guidebooks.

I tried using that format, until I pulled a text file into Excel and it changed all the phone numbers into "real numbers" and deleted terminal zeros. Excel also has this annoying habit with IP addresses, changing 10.0.0.10 to 10.0.0.1. I can't find a way, in the \*import\* function, to define these numbers as "text" so that Excel will leave them alone upon import. Sigh.

---

## **Sweden's public radio reportedly bans SETI from office computers**

Declan McCullagh <declan@well.com>  
*Thu, 08 Nov 2001 15:22:14 -0500*

SETI homepage:  
<http://setiathome.ssl.berkeley.edu/>

Date: Thu, 08 Nov 2001 21:10:05 +0100  
To: declan@well.com  
From: Ulf Hedlund <guru@slideware.com>  
Subject: Swedish national radio bans SETI software

Conspiracy theory has reached the state owned public service radio in Sweden, "Sveriges Radio" (www.sr.se). They have banned all use

of the SETI software and says that three of the technicians from the IT department are going to be relocated. According to the head of human resources, Per Thorsell, this is due to the fact that they don't know if the software is actually performing search for extraterrestrial life. "The software could be used by some service for other purposes, e.g., calculation of missile ballistics", he says.

<http://www.sr.se/ekot/index.asp?article=22761> [in Swedish; translation tinkered slightly after consulting Ulf Lindqvist, who suggests they should be equally paranoid about other black-box software they might be running. PGN]

To subscribe to Politech: <http://www.politechbot.com/info/subscribe.html>

This message is archived at <http://www.politechbot.com/>

---

## ✶ Random failures (Re: Bank Canada, Sokskiewicz, [RISKS-21.73](#))

Andrew Brydon <[andrew@isbjorn.demon.co.uk](mailto:andrew@isbjorn.demon.co.uk)>

*Tue, 6 Nov 2001 22:31:18 +0000*

>I think that sometimes we are better off accepting such "random" occurrences

Rather we should be analysing our systems for random failures and interactions due to these random occurrences, designing out or mitigating to limit the effects of such failures. To do any less may be unprofessional, and in many cases illegal.

>Sometimes I feel that RISKS readers expect to live in a perfect world.

I think we should expect all reasonable care to be taken over developing and implementing the systems which we use, as for any other consumer product or service. The difference with, say a toaster, is that there are far fewer interactions and controls to consider, but we still expect it to turn bread to toast without error.

Andrew Brydon, Systems & Software Safety Analyst, Lancashire, UK

---

## **⚡ Re: Another SRI-wide Power Outage**

"Marcus L. Rowland" <mrowland@ffutures.demon.co.uk>

*Tue, 30 Oct 2001 23:02:37 +0000*

A couple of weeks ago I spent three hours trying to find out why one of our laboratories (see various previous comp.risks digests) was tripping out its circuit breakers again, despite the system having been overhauled.

We eventually realised that someone had put a box of equipment down on top of a stool that wobbled slightly, so that it pressed against the emergency cut-out button whenever someone brushed past it...

Marcus L. Rowland

<http://www.ffutures.demon.co.uk/>

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

[VERY OLD problem. In the Multics days in the later 1960s at

Bell Labs,  
sitting down in a particular chair in the computer room would  
often  
crash the system, due to the under-floor wiring. PGN]

---

## **⚡ Re: Kids' learning game site becomes porn site ([RISKS-21.73](#))**

"Daniel P. B. Smith" <dpbsmith@bellatlantic.net>

*Mon, 05 Nov 2001 20:11:49 -0500*

In the interest of becoming a well-informed netizen, I took a  
look at

<http://www.moneyopolis.org> and <http://www.moneyopolis.com>.

Imagine my

disappointment^h^h^h^h^h^h^h^h^h^h^h^h^h^h^h^h relief, to find  
that as of

11/5/2001 these sites appear to be ... an online interactive  
children's

game produced as a public service by Ernst and Young.

Daniel P. B. Smith <dpbsmith@world.std.com>

[Quite a few RISKS readers noted this. So, either the  
WashPost and NYT

(which ran its own story) got it wrong, or E&Y quickly  
repaired its image

by re-acquiring the .org domain -- presumably at an indecent  
markup. PGN]

---

## **⚡ Re: Kids' learning game site becomes porn site ([RISKS-21.73](#))**

Ian Young <ian@iay.org.uk>

*Tue, 6 Nov 2001 09:58:17 -0000*

You won't be surprised to hear that Ernst & Young (no relation) are not the only people to have been affected by this scheme. I got some moderately irate E-mail recently from users of a small site I run because one of the sites I had linked to had apparently converted to a porn site in the way the \*Post\* describes.

However, in this case:

- \* the registration was by a different company: someone out of Tbilisi, Georgia instead of Yerevan, Armenia.

- \* The new site contained a single page containing an advertisement for "Euro Teen Sluts", plus half a dozen post-close pop-ups for similar sites, but also offered to sell you the domain name in question!

Obviously, buying up random dead domains is a cheap way of getting advertising space, as long as you don't care who sees the adverts in question.

Risk 1: links are sometimes seen as endorsements. That's a problem for me, but it is presumably also a problem for people like Google, whose rating system depends on seeing that particular sites are linked to by other sites. I wonder how they cope with this? I can see that they do, because the site I linked to still has a lot of links to it, but no longer appears in a Google search with any of the obvious keywords...

Risk 2: automatic link checkers will tell you there is something there, but

they won't tell you what it is. You actually have to visit your links once in a while to check they haven't turned into something else.

---

**✶ Re: Kids' learning game site becomes porn site ([RISKS-21.73](#))**

"Paul Bowers" <pbowers@PipingDesign.com>

*Mon, 5 Nov 2001 21:11:49 -0500*

On a similar theme, one of my visitors pointed out to me that a link from my site was now resolving to some cyber-babe page. Apparently, [exicom.org](#) recently changed owners.

The articles I had linked from the site were good technical pages.

---

**✶ Re: DeCSS is Speech (Tyre, [RISKS-21.73](#))**

Amos Shapir <amos@sela.co.il>

*Tue, 06 Nov 2001 14:37:22 +0200*

May I point out that the original purpose of ALGOL -- the granddaddy of all structured programming languages -- was to create a common set of notations which would enable people to converse about algorithms. ALGOL code was not meant to be compiled into executable object code, and its first specification (of 1960, IIRC) had no defined means for I/O.

Amos Shapir

## **⚡ Re: DoS attack on Mac OS9 (Gat, [RISKS-21.73](#))**

"William Kucharski" <kucharsk@mac.com>

*Sun, 11 Nov 2001 07:31:51 -0700*

The risk in MacOS 9 is not surprising, and not really a RISK. Not unless you're expecting the Multiple Users feature of MacOS 9 to provide anything more than rudimentary security.

Sure, you can change passwords if you have physical access to the machine.

You can also boot any Mac with a MacOS 9 CD and completely circumvent all protection.

The biggest RISK here is believing a feature meant largely to provide different environments for different family members or to prevent clueless users from damaging the system (i.e. dragging crucial system control panels or extensions to the trash) provides any TRUE degree of security...

William Kucharski <kucharsk@mac.com>

---

## **⚡ Re: DoS attack on Mac OS9 (Gat, [RISKS-21.73](#))**

Carl Maniscalco <camannospam@earthlink.net>

*Sun, 11 Nov 2001 16:51:33 -0800*

The Multiple Users control panel in OS 9 *\*is\** a pretty ugly hack

but the security risk isn't quite as bad as Mr. Gat makes it out to be. To effect a password change that would "render that machine useless," the malicious user would have to gain access to a Mac where someone has already logged on to the admin account. In my opinion, anyone who leaves a computer unattended in that state in an insecure environment probably deserves whatever he gets.

Carl Maniscalco, Deus Ex Macintosh, Mac Consultants, San Diego, CA



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 21: Issue 75

**Monday 19 November 2001**

## Contents

- [Feds make record counterfeit software seizure](#)  
[NewsScan](#)
  - [Google freely giving out your phone number and home address](#)  
[Derek Ziglar](#)
  - [Researchers probe Net's 'dark address space'](#)  
[Kevin Poulsen via Dewayne Hendricks and David Farber](#)
  - [A large risk of national ID cards](#)  
[Adam Shostack](#)
  - [Re: Programming error scrambles election results](#)  
[Hamish Marson](#)  
[Phil Kos](#)
  - [Re: DoS attack on Mac OS9](#)  
[Erann Gat](#)
  - [IP: Announcing URIICA - For the Sake of Internet Users Everywhere](#)  
[PGN](#)
  - [REVIEW: "Internet and Computer Ethics for Kids", Winn Schwartau](#)  
[Rob Slade](#)
  - [Info on RISKS \(comp.risks\)](#)
-

## **⚡ Feds make record counterfeit software seizure**

"NewsScan" <newsscan@newsscan.com>

*Mon, 19 Nov 2001 08:04:38 -0700*

California law enforcement officials made the largest seizure of counterfeit software in U.S. history, estimated to be worth about \$100 million. The products, which originated in Taiwan, included about 31,000 high-quality copies of Microsoft's Windows Millennium Edition and 2000 Professional operating systems and tens of thousands of copies of Symantec security software. "They look so good that the purchaser would not know it was counterfeit," said Los Angeles County Sheriff Lee Baca. Some of the bogus discs even carried the "Do not make illegal copies of this disc" warning. Authorities have arrested three people on bribery conspiracy and smuggling charges, and another has been charged with state violations of counterfeiting a registered trademark. [AP 16 Nov 2001; NewsScan Daily, 19 Nov 2001 <http://news.excite.com/news/ap/011116/20/counterfeit-software>]

---

## **⚡ Google freely giving out your phone number and home address**

"Derek Ziglar" <dziglar@yahoo.com>

*Tue, 13 Nov 2001 09:24:58 -0500*

If you are in the USA, try searching in Google for your name, followed by your city, state or zip code--such as: Bob Smith Alaska. The

first  
results you get may well be your home phone number, home  
address, and a  
link to a map (in some cases with a satellite photo of your  
house, too).

The RISKS are staggering that this type of personal information  
is being  
automatically given out to people that weren't even asking for  
it. Sure,  
they were looking for some information about you. But cross  
linking data  
across purposes (web search versus telephone lookup) is one of  
the biggest  
privacy risks of the modern connected database age. It rapidly  
becomes  
one-stop shopping for everything anyone would want to know about  
you--whether they were asking for all that detail or not!

In addition, Google does not provide any obvious mechanism to  
request  
removal from this telephone listing.

Derek Ziglar (city and state withheld for obvious reasons)  
dziglar@yahoo.com

---

## **✶ Researchers probe Net's 'dark address space' (From Dave's IP)**

David Farber <dave@farber.net>  
*Thu, 15 Nov 2001 15:53:54 -0500*

>From: Dewayne Hendricks <dewayne@warpspeed.com>

Researchers probe Net's 'dark address space'

By Kevin Poulsen

Posted: 15/11/2001 at 02:30 GMT

<<http://www.theregister.co.uk/content/55/22850.html>>

Broadband customers and US military systems are the most common victims of an online phenomenon researchers have dubbed "dark address space," which leaves some 100 million hosts completely unreachable from portions of the Internet.

For a variety of reasons ranging from contract disputes among network operators to simple router mis-configuration, over five percent of the Internet's routable address space lacks global connectivity, according to the results of a three-year study by researchers at Massachusetts-based Arbor Networks, to be released Tuesday.

"Popular belief holds that the Internet represents a completely connected graph," says Craig Labovitz, Arbor Networks' director of network architecture. "It turns out that's just not true."

Anecdotal evidence has long hinted at the existence of dark address space, but the researchers shed light on the subject by continuously gathering and analyzing core routing tables for three years. In the end, they found that for much of the Internet, the shortest path between two points doesn't exist.

The most common factors contributing to dark address space: aggressive route filtering by network operators seeking to ease the load on equipment, and accidental mis-configuration. US military sites frequently fall into the shadow zone because they often occupy neglected 'Milnet' address blocks dating back to the Internet's stone age. Why cable modem customers also top the list remains one of the unsolved

mysteries in the project, says Labovitz, who describes the research findings as preliminary.

#### Murky Crime

Despite the large number of hosts that fall into the partitioned space, the phenomenon is generally not noticeable to average Internet users because most Netizens only use a tiny portion of the Net. "Most people access five or ten web sites," Labovitz says.

The study was conducted by Labovitz, Michael Bailey and Abha Ahuja. [...]

[For IP archives see:

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

---

## **A large risk of national ID cards**

Adam Shostack <adam@zeroknowledge.com>

*Mon, 12 Nov 2001 09:58:12 -0500*

(In response to <http://www.csl.sri.com/neumann/insiderisks.html>)

I believe that there is an important risk, that of reliance, that will accompany a high-tech national ID card. Every terrorist commits their first act of terrorism at some time in their life, and before that time, they cannot be any database of known terrorists.

Once you start issuing cards, people will start relying on 'identity verification' rather than threat management. We'll see people

relying on background checks [1] rather than xrays. We'll see special lines for frequent fliers, who are 'known trustworthy.' They differ from pilots and flight crew in that they don't run into co-workers who can notice and react to strange behavior before the flight. If you want to keep knives and guns off of planes, the answer lies in xrays, magnetometers, and other searching technology, not in believing that you know who's who. Many of the national id card risks come from a layer of indirection from the real problem, which is not "Is Alice trusted," but, "Is the person in front of me trusted?" National ID cards not only do nothing to solve this problem, they distract us from attempting to solve it.

[1] See the last para of

<http://www.spectrum.ieee.org/WEBONLY/special/sept01/idcards.html>

---

## ✈ Re: Programming error scrambles election results ([RISKS-21.74](#))

Hamish Marson <hamish@travellingkiwi.com>

*Mon, 12 Nov 2001 14:37:21 +0000*

The question remains. why oh why do companies insist on believing that the programmer is the best person to check, test and validate a piece of software that THEY have written.

Not withstanding blatant bugs in the implementation of the logic, a tester

will only test (Baring bugs in their testing of course :) what they anticipate the inputs to be. If the same people do the testing that did the programming, you are potentially missing out on whole swathes of input, because the same person doesn't realise they should be testing something they never thought of in the first place...

Personally I like to think that anything I written isn't ready for prime time until at least one other person who UNDERSTANDS THE PROBLEM BEING SOLVED has had a chance to throw their data at it & verify if valid data comes out the other end.

---

## **✶ Re: Programming error scrambles election results ([RISKS-21.74](#))**

Phil Kos <PhilK@solthree.com>

*Fri, 16 Nov 2001 18:20:02 -0800*

> .... a veteran county employee claimed to have tested his code, but  
> apparently had not actually done so.

Is it just me, or has anyone else noted that the two primary RISKS here are developers "testing" their own code and managers who think that software development is that trivial? I don't care how experienced a developer is, nobody (not even I! ;) can be relied on to find their own bugs. I would have certainly chastised the developer for not doing his job well enough, but I wouldn't had fired him. Instead I would have fired the people

above him in  
the county bureaucracy who feel that critical software doesn't  
need to be  
tested--they're the truly dangerous ones here, and they're  
presumably still  
conducting business as usual now that they've sacrificed their  
scapegoat.

[Testing by other folks is of course not sufficient. But even  
more

critical, design and code reviews are also useful in trying to  
detect

Trojan horses, trapdoors, etc., placed intentionally by  
developers with

the expectation that they would facilitate rigging elections.

PGN]

---

## ✶ Re: DoS attack on Mac OS9 ([RISKS-21.73-74](#))

Erann Gat <gat@flownet.com>

*Mon, 12 Nov 2001 14:14:53 -0800 (PST)*

Another masterful display of editorial subtlety from our  
esteemed moderator:

From: "William Kucharski" <kucharsk@mac.com>

> The risk in MacOS 9 is not surprising, and not really a RISK.  
Not

> unless you're expecting the Multiple Users feature of MacOS 9  
to provide

> anything more than rudimentary security.

From: Carl Maniscalco <camannospam@earthlink.net>

> In my opinion, anyone who leaves a computer unattended in that  
state in

> an insecure environment probably deserves whatever he gets.

So on the one hand the security is so weak that the only risk is that users might be foolish enough to think that the feature is something more than a simple facade, but on the other hand the security is so strong that we are justified in blaming the victims of maliciousness or, more to the point, typos, for not being able to log in to their own machines any more.

I really don't want to belabor this, but both of these respondents seem to have missed the point: I never meant to suggest that the OS9 multiple users feature should be taken seriously as a security measure. That's why the subject of my post was "DoS attack on Mac OS9" and not "Security weakness in Mac OS9". The problem is not that security is weak (well, that's a problem too, but not the one I was talking about) but that the password can be changed without knowing the old password and without confirming the new password (which is, of course, not echoed on the screen). I'll grant that in reality attacks from malicious users are probably not a major concern, but if there's only one account on your machine and you decide to change its password then you had better type it in very, very carefully.

Erann Gat <gat@flownet.com>

---

**⚡ IP: Announcing URIICA - For the Sake of Internet Users Everywhere**

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

Wed, 14 Nov 2001 07:55:43 -0500

Announcing "URIICA" - Union for Representative International  
Internet

Cooperation and Analysis

<http://www.uriica.org>

Lauren Weinstein

Peter G. Neumann

David J. Farber

November 13, 2001

An Open Letter to the Global Internet Community

== Executive Summary ==

The Internet has become too important for its development, management, security, and other critical aspects to continue largely on an ad hoc basis. Internet-related issues, which now impact our world and lives in a vast number of ways, are usually approached in isolation from one another by existing organizations, and often in parochial and non-representative ways.

We submit that a new organization is needed, created specifically to provide guidance relating to Internet functions and issues on an international and truly representative basis. Such an organization could also help establish confidence that the Internet exists to benefit people everywhere, not merely commercial and other special interests. We offer URIICA -- Union for Representative International Internet Cooperation and Analysis -- as a

possible first step towards building such a future.

-----

URIICA - Union for Representative International Internet  
Cooperation

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

In the more than thirty years since its genesis, the technology of the Internet has evolved from a little-known experiment to a major part of the world's infrastructures, with massive impacts throughout nearly every aspect of our cultures and lives -- from government to commerce, and from education to entertainment. Over the decades, innumerable individuals and informal groups have labored to make the Internet what it is today. Formal organizations have also played crucial roles, including ISOC, IETF, and ICANN, to name only three among many.

But while the technical evolution of the Internet has been extraordinary in many respects, the ways in which the Internet is "managed" appear to be increasingly ill-suited in terms of overall planning, coordination, security, reliability, privacy, and numerous other key attributes. Of equal concern is the perception that Internet development has become largely hostage to well-heeled, vested interests. There are few and ever-decreasing opportunities for meaningful input on Internet issues from nonprofit organizations or ordinary Internet users without significant financial resources.

These problems have been exacerbated by the historically

isolated nature of many organizations working on Internet issues. There is a tendency for each such group to concentrate mainly on their own interests, with little coordination with other groups or persons who may have different points of view. There are also indications that some organizations have moved to extend their influence beyond their true competencies, and that those who have come to wield de facto power over controversial Internet-related issues may do so without a due consideration of international concerns, true representation, or even ordinary fairness.

In the People For Internet Responsibility (PFIR) "Statement on Internet Policies, Regulations, and Control" [1], and "PFIR Proposal for a Representative Global Internet Policy Organization" [2], it has been suggested that the creation of a new international organization specifically to address these issues is a necessary step to successfully bring the Internet out of the age of turf wars and amateur theatrics into its appropriate role as a critical resource for the \*entire\* world and \*all\* of its peoples. Of course, moving from theory to practice is often difficult, particularly when dealing with the founding of organizations that must tackle controversial issues.

However, the rising importance of the Internet and the continuing decline in public confidence regarding its operations suggest that action is urgently needed now. It is with this in mind that we offer "URIICA" - Union for Representative International Internet Cooperation and Analysis

(<http://www.uriica.org>). The name may be long, but its premise and goal is basically simple:

The Internet should be dedicated to the needs and well-being of people all over the world, in a truly representative and fair manner.

We offer URIICA as a forum for discussion, planning, and for building a framework towards accomplishing this goal, by bringing together in a \*representative\* manner an \*international\* group of diverse persons, organizations, and other groups who have commitments to the future of an open Internet. These participants will not only encompass commercial interests, but also a wide range of nonprofit organizations, educational institutions, government agencies, individual Internet users, and anyone else who is willing to sit down and work for the common good. We visualize URIICA as being a very big tent indeed, with a structure created from the ground up to encompass both domestic and international concerns, based upon balanced, fair representation for everyone involved.

We do not present URIICA as a *fait accompli*. There are innumerable details to be considered. But we hope URIICA will be a useful vehicle to bring together many persons and organizations for the work, debate, and serious long-term planning that is desperately needed. The Internet needs vision and dedication to be a beacon of hope for the future, and not merely a hi-tech mediocrity.

If you're interested in helping, or have other comments, we'd very much appreciate hearing from you. General comments and questions can be e-mailed to:

uriica@uriica.org

Please also feel free to call Lauren Weinstein on +1 (818) 225-2800 (M-F 9:30 AM - 5:30 PM Pacific Time) if you wish to discuss this effort.

If you'd like to join a (low-volume) e-mail list dedicated to URIICA and these issues, please send the message text:

subscribe

as the first text in the body of a message (the "Subject" field doesn't matter) to:

uriica-request@uriica.org

Over two millennia ago, the Greek mathematician Archimedes exclaimed "Eureka!" ("I have found it!") when he solved a vexing mathematical problem. We hope that URIICA can be of value in helping us all move towards solving many of the important problems of the Internet that we face both today and tomorrow. Thank you, and our best wishes to you all.

[1] PFIR Statement on Internet Policies, Regulations, and Control

<http://www.pfir.org/statements/policies>

[2] PFIR Proposal for a Representative Global Internet Policy Organization

<http://www.pfir.org/statements/proposal>

Sincerely,

Lauren Weinstein

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

Tel: +1 (818) 225-2800

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

Co-Founder, Fact Squad - <http://www.factsquad.org>

Co-Founder, URIICA - Union for Representative International Internet

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

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

Member, ACM Committee on Computers and Public Policy

Peter G. Neumann

neumann@pfir.org or neumann@csl.sri.com or neumann@risks.org

Tel: +1 (650) 859-2375

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

Co-Founder, Fact Squad - <http://www.factsquad.org>

Co-Founder, URIICA - Union for Representative International Internet

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

Moderator, RISKS Forum - <http://risks.org>

Chairman, ACM Committee on Computers and Public Policy

<http://www.csl.sri.com/neumann>

David J. Farber

farber@cis.upenn.edu

Tel: +1 (610) 304-9127

Member of the Board of Trustees EFF - <http://www.eff.org>

Member of the Advisory Board -- EPIC - <http://www.epic.org>

Member of the Advisory Board -- CDT - <http://www.cdt.org>

Member of Board of Directors -- PFIR - <http://www.pfir.org>

Co-Founder, URIICA - Union for Representative International Internet

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

Member of the Executive Committee USACM  
<http://www.cis.upenn.edu/~farber>

(Affiliations shown for identification only.)

---

## ★ REVIEW: "Internet and Computer Ethics for Kids", Winn Schwartau

Rob Slade <rslade@sprint.ca>  
*Thu, 15 Nov 2001 08:03:15 -0800*

BKINCMEK.RVW 20010815

"Internet and Computer Ethics for Kids", Winn Schwartau, 2001,  
0-9628700-5-6, U\$15.95/C\$24.95

%A Winn Schwartau www.nicekids.net winns@gte.net  
%C 11511 Pine St. N., Seminole, FL 33772  
%D 2001  
%G 0-9628700-5-6  
%I Inter.Pact Press  
%O U\$15.95/C\$24.95 727-393-6600 fax: 727-393-6361  
%P ~150 p.  
%T "Internet and Computer Ethics for Kids"

Computer ethics can be a very frustrating field. Professional organizations appear to have abandoned the area: they seem to have given up on the idea of "codes of ethics" and now prefer to write "codes of conduct." "Values education" has progressed very little in the last thirty years. All of us seem to be the disciples of Kohlberg, and assume that by sitting around discussing ethics, moral dilemmas, and scenarios, we will all somehow become moral individuals.

And that's for the adults.

For kids, the task is even more important, and much more difficult. Maybe it's impossible. But it is good to see that someone has at least given it a try. I don't agree with everything Winn has done, but he has produced a valuable and helpful tool. I hope that a great many people try it out, and, if it needs tuning, feed ideas back to improve it.

This volume is a tool, and must be seen as such to be valued. Schwartau has, probably wisely, not attempted to provide a full examination of ethical theories or systems. The chapters are all very short: they are introductions, not expositions. (As Blaise Pascal famously noted, it takes much longer, and much more work, to write a short piece than a long one.) The text is generally possible for the sixth grade reader, and is backed up with a short section on relevant ideas from the law, topics to think about and discuss, and resources for further study and research.

Unfortunately, the work starts out weakly. The introduction is vague. Seemingly the book is addressed to everyone. The preface also states that the book has questions, but no answers. A second introduction is more personal, but no clearer as to the intent of the text.

Chapter one states that there are no rules, and then lays out some rules. Aside from the contradiction, which may be too subtle for the younger end of the audience, but which will probably be picked up by the later teens, relativism makes it difficult to discuss ethics at all. To the question of

what ethics are, chapter two has little explanation except to say that they are the "little voices." A brief Internet history is probably supposed to point out that the Internet has grown too fast for formal regulation, in chapter three. Chapter four starts out by raging against stereotypes of all kinds, and then stereotypes the media. The text also tersely outlines various types of hackers. Chapter five is a scenario, a rather simplistic story of a young person who is very clearly dealt with unfairly by "the Establishment," whose only possible recourse is to make unauthorized alteration of data on a computer.

The material starts to get stronger as it becomes more specific. Passwords, and the needs for strong ones, are discussed in chapter six. Graffiti is equated with web page defacement in chapter seven. Phone phreaking, war dialing, and anonymity are defined in eight to ten. Malware, viruses and trojan horse programs, are covered in chapters eleven and twelve. Chapters thirteen and fourteen deal with spoofing and spam. Chapter fifteen points out that you have no idea whether what is said on the net is true, which leads to discussions of scams, online business, and rumours in sixteen to eighteen. Stealing, in chapter nineteen, leads to examinations of software piracy and plagiarism.

Chapters twenty two to twenty five look at the more ambiguous topics of social engineering, flaming, meeting people, and stalking. Technical subjects, digital special effects and eavesdropping, get a brief

look in  
chapters twenty six and twenty seven.

The topics get harder as chapter twenty eight deals with pornography, then two chapters on privacy, another on monitoring, and ratting on others.

Although the topics could be presented in various sequences, it might have been better to place chapter thirty three, discussing ethics and the law, closer to chapter two. But it is also a good lead-in to civil disobedience and hacktivism, in chapter thirty four.

The review of personal responsibility, in chapter thirty five, is very good.

"Computer Police," in thirty six, deals mostly with law enforcement concerns, with a brief mention of vigilantism. An interesting juxtaposition with chapter thirty seven, on getting caught.

Chapter thirty eight, asks who makes the rules, but deals primarily with the home and who is in charge. Again, making ethical decisions, in thirty nine, is good, but should be related to two and thirty three.

Although it finishes off the book, chapter forty, and cyber-parenting, is the introduction for parents and teachers. It is quite realistic and balanced.

A final set of pages is probably an important part of the book. A set of lined pages, they are important exercises for self-examination, headed with

"My Personal CyberEthics," "My Family's CyberRules," "My Friends' CyberEthics," "CyberRules at My Friends' House," "CyberRules at School,"

"What My Parents Need to Learn," "What My Teachers Need to Learn," "My Company's CyberEthics and Rules," and "What I think I Need to Learn."

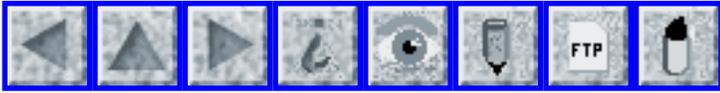
I won't give this book to my grandchildren, even though the oldest would probably be able to read a good part of it. But I will give it to their mothers.

Not being a marketroid, I will not say that this book is a "must have" for anyone with kids. Unlike many other books, and like many computer technologies, it must be used to be of any value. Parents can't simply present it to their children and forget it: to do so would be to teach that ethics are not important. If you want to get anything out of this work, you will have to read it with your kids, or give it to them to read, and discuss it with them. It can be read in an afternooon, but shouldn't be. The material should be taken a chapter at a time, perhaps once a week, perhaps at even longer intervals. It may take years to finish this slim volume (by which time all the URLs may be 404). As the adult you will have to be patient, and accept that the discussions may not proceed in straight lines, as you think they should.

The end result, though, should be worth it. You'll have ethical kids.

copyright Robert M. Slade, 2001 BKINCMEK.RVW 20010815  
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 21: Issue 76**

**Tuesday 20 November 2001**

## Contents

- [Many Federal computers fail hacker test](#)  
[PGN](#)
- [800 directory "assistance" redirecting calls](#)  
[Brett Glass via Dave Farber](#)
- [Paperless billing and opening a bank account](#)  
[Ian Chard](#)
- [Microsoft IE Javascript cookie disclosure vulnerability](#)  
[Max](#)
- [Metro Headline: "Windows hacked in hours"](#)  
[Chris Leeson](#)
- [Windows XP accounts by default are administrator, with no password](#)  
[Jonathan Epstein](#)
- [Toaster failures](#)  
[Tom Hackett](#)
- [Trick the user with Outlook XP and possibly others](#)  
[Nathan Neulinger](#)
- [Re: Dates in Visual Basic](#)  
[Nick Brown](#)
- [Re: Excel and non-decimal dots](#)  
[Mark Brader](#)

- [Porn spam being sent in my name](#)  
[Nickee Sanders](#)
  - [Re: Kids' learning game site becomes porn site](#)  
[Dan Fandrich](#)  
[Malcolm Pack](#)
  - [Computers & bureaucracy help spread of foot & mouth disease](#)  
[Charles Shapiro](#)
  - [Re: Another SRI-wide power outage](#)  
[Kelly Bert Manning](#)
  - [REVIEW: "White Hat Security Arsenal", Aviel D. Rubin](#)  
[Rob Slade](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

## ✶ Many Federal computers fail hacker test

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

*Fri, 16 Nov 2001 13:15:12 PST*

The latest quarterly computer-security report card put together by Congressman Steve Horn's House Reform Committee government efficiency subcommittee and the GAO and OMB gives the government an F grade (down from a D- a year ago), based on lax protection of federal computer networks against hackers, terrorists, and others. Two-thirds of the federal agencies flunked this time, including the departments of Defense, Commerce, Energy, Justice, Treasury, Agriculture, AID, Education, Health and Human Services, Interior, Labor, Transportation, Small Business, and Veterans Affairs. The B+ given to the National Science Foundation was tops, with Social Security getting a C+ and NASA C-. As expected, the GAO found systems

with no passwords, with ``password'' as password, and with unencrypted accessible password files. [Source: AP Online via COMTEX, 9 Nov 2001, PGN-ed]

---

## ✶ IP: 800 directory "assistance" redirecting calls

Brett Glass <brett@lariat.org>  
*Fri, 16 Nov 2001 12:03:56 -0700*

[From David Farber's IP  
<http://www.interesting-people.org/archives/interesting-people/>]

IPers might be interested in something that happened to me today. I am planning a trip to Denver, and wanted to stay at the Adam's Mark hotel. Not knowing the toll-free number for the chain, I called 800-555-1212 (toll-free information) to ask for the number.

"Toll-free directory assistance, powered by TellMe!" said a recorded message. I told the recording that I wanted the number of the Adam's Mark.

However, instead of receiving the correct number for the chain (listed on their Web site as 800-444-ADAM), I received a different number: 800-866-5038. This number was not actually the number of the hotel chains, but rather that of a third party room wholesaler in Orlando, Florida.

Calling the correct number, I confirmed that the hotel chain had no idea

that calls were being diverted to a third party.

As the economy continues into recession, we are likely to see more and more instances of "customer hijacking," in which companies -- perceiving their markets as a zero sum game -- work to grab customers from one another in any way possible, regardless of ethics. "Slamming," and the hijacking of ISPs' DSL customers by ILECs, are only two of the many other hijacking techniques which are now becoming prevalent in slowly growing, or shrinking, markets.

Brett Glass

---

## **✶ Paperless billing and opening a bank account**

Ian Chard <ichard@cadence.com>

*Fri, 16 Nov 2001 09:53:48 +0000 (GMT)*

I recently opted for paperless (i.e., e-mailed) billing from both British Telecom and my electricity provider, and am now finding that's it's much harder for me to convince some financial institutions of my identity.

Many banks insist on a "recent utility bill" [1] as partial proof of ID, and the application processing staff seem to be trained to reject anything that looks remotely unusual. Unsurprisingly, they rejected a printout of my "e-bill" as well as my (paper) gas bill, as I'm not on mains gas and they hadn't heard of the supplier. The only way I could satisfy them was to ask

the electricity company to provide a printed copy of my bill (something they tried to charge me for).

Ironically, this was an application for a paperless account!

[1] Of course, this means that the bank have an implied trust in the utility companies to do some checking of their own.

Ian Chard, Unix Systems Administrator, European IT, Cadence Design Systems Ltd  
The Alba Campus, Livingston, Scotland EH54 7HH +44 (0)1506 595019

---

## ⚡ Microsoft IE Javascript cookie disclosure vulnerability

Max <max7531@earthlink.net>  
*Thu, 15 Nov 2001 12:58:33 -0800*

A flaw was discovered in the way Internet Explorer's about: protocol handles javascript requests, enabling a malicious web site to gain access to cookie information on the client's hard drive.

<http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=discussion&id=3513>

MS has set the record for the fastest patch issuance:

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms01-055.asp>

I wonder which correlation is better: patch issue time vs. possible publicity problems, patch issue time vs. problem solvability, or patch issue

time vs. problem severity?

---

## ✶ Metro Headline: "Windows hacked in hours"

"Chris Leeson" <CHRIS.LEESON@london.sema.slb.com>

*Fri, 16 Nov 2001 10:49:44 -0000*

The 01 Nov 2001 edition of Metro (a free newspaper in London) had this article on the front page, which began as follows.

"Hackers cracked and copied Microsoft's much-lauded new Windows software within hours of its launch, it emerged last night.

Black market copies of the supposedly uncrackable Windows XP, which took 16 years to develop, are already on sale for 5 pounds."

After making a reference to Microsoft's advertising, the article goes on to mention that:

- Hackers were exploiting two "simple security loopholes"
- One of these was a security key "now widely available on the Internet"
- Microsoft had admitted that illegal copies were already on sale in China.

Not being an expert on such things, I cannot comment on the "security loopholes", but I thought that the "16 years to develop" was a classic!

## **✶ Windows XP accounts by default are administrator with no password**

Jonathan Epstein <Jonathan\_Epstein@nih.gov>

*Thu, 15 Nov 2001 16:00:44 -0500*

The Register has an entertaining article:

<http://www.theregister.co.uk/content/4/22863.html>

which, among other things, points out Microsoft Knowledge Base article Q293834:

<http://support.microsoft.com/support/kb/articles/Q293/8/34.ASP>

whose summary reads:

"After you install Windows XP, you have the option to create user accounts.

If you create user accounts, by default, they will have an account type of Administrator with no password."

---

## **✶ Toaster failures (Re: Random failures, Brydon, [RISKS-21.74](#))**

Tom Hackett <ThHackett@vassar.edu>

*Mon, 12 Nov 2001 22:34:03 -0500*

> The difference with, say a toaster, is that there are far fewer interactions and controls to consider, but we still expect it to turn bread to toast without error.

I'd like to know where Andrew gets his toasters! I have been married for over thirty years, and we average about five years per toaster (mean time between catastrophic failures). I have yet to own a toaster that will reliably produce evenly browned toast day after day. The more

sensors and other gadgets the toaster has, the less likely it will be able to produce something between soft white and charred black. (Well, this actually supports Andrews overall point, I suppose.)

I've noticed recently that some toasters will actually not turn off the heating elements until the toast is successfully "popped," with the result that if the bread should get stuck, the risk of fire is significant. I wonder that this hasn't caused become a recognized safety issue.

The only toaster in our house that works satisfactorily is the one given to my in-laws for their wedding fifty-three years ago. It has no "doneness" sensors and a completely mechanical timer.

---

## **⚡ Trick the user with Outlook XP and possibly others**

"Neulinger, Nathan" <nneul@umr.edu>  
*Mon, 12 Nov 2001 14:11:24 -0600*

Summary: system messages in the bar above the headers

I recently saw a couple messages from a friend that had this yellow bar at the top of the message (same place as outlook sticks other system messages, like that annoying stuff about extra line breaks, and the "You have replied to this message" comments)

The message said:

(i) Your mailbox is corrupt. Upgrade your mail software.

Now, obviously, I was a bit disturbed by this. Tracking it down, it is the "X-Message-Flag" mail header.

Seems to me it can be quite dangerous to allow a remote user to cause messages to be displayed on your mail client that appear to be generated by the system. (Think about what stupid users do when people send them forwards saying to do stuff.)

(For reference, I don't use Outlook by choice, and at least I'm running it under VMWare on linux.)

Nathan Neulinger, Computing Services, University of Missouri - Rolla  
1-573-341-4841 nneul@umr.edu

---

## ⚡ Re: Dates in Visual Basic ([RISKS 21.74](#))

Nick Brown <Nick.BROWN@coe.int>  
*Mon, 12 Nov 2001 09:09:50 +0100*

```
> #2001-11-08# becomes #11/8/2001# (2001-11-08)
> #11/8/2001# becomes #11/8/2001# (2001-11-08)
> #8/11/2001# becomes #8/11/2001# (2001-08-11)
> #15/11/2001# becomes #11/15/2001# (2001-11-15)
```

```
> The first has reduced the comprehensibility of the code. The
second and
> third give no feedback that they're not conforming to the
current locale.
> The last two show that VB is not even being consistent in its
parsing.
```

Oh, but it *\*is\** being consistent, if you assume that the algorithm is:

- Find a number which could only be the month
- Find a number which could only be the day
- If there is ambiguity, assume the user typed the date in mm/dd order

Now, of course, this is so wrong as to be bordering on the criminally

negligent (not for nothing is MS sometimes known in France as "Crimosoft").

It shows what can happen even if you put millions of dollars into internationalisation (as MS undoubtedly has), but then hire a short-term

contractor who has never set foot outside the US and let him or her write

date validation code unsupervised.

(I remember about 15 years ago seeing a Lotus 1-2-3 manual which proudly

claimed that the program accepted various date formats, including "the international standard, mm/dd/yy")

---

## ✶ Re: Excel and non-decimal dots ([RISKS-21.74](#))

Mark Brader <msb@vex.net>

*Mon, 12 Nov 2001 09:17:53 -0500 (EST)*

These replies were directed to me.

```
> From mark.lomas@tmalomas.com Mon Nov 12 07:57:57 2001
> From: "Mark Lomas" <mark.lomas@tmalomas.com>
> To: <msb@vex.net>
> Cc: <magical@rahul.net>, <davidhecht@prodigy.net>
> Subject: Re: Excel and non-decimal dots
> Date: Mon, 12 Nov 2001 12:54:09 -0000
```

>  
> In [Risks Digest 21.74](#) you wrote:  
>  
> Date: Wed, 7 Nov 2001 13:43:25 -0500 (EST)  
> From: msb@vex.net (Mark Brader)  
> Subject: Excel and non-decimal dots  
> >  
> > \* From: magical@rahul.net  
> > \* Newsgroups: alt.usage.english  
> > \* Subject: Re: Telephone Area Code  
> > \* Message-ID: <7bqiutgjqqgl1tu29qd6ak615c14pbcfavo@4ax.com>  
> > \* Date: Wed, 07 Nov 2001 17:07:08 GMT  
> >  
> > On Wed, 07 Nov 2001 07:54:15 GMT, in alt.usage.english, David  
> > Hecht <davidhecht@prodigy.net> created  
> >  
> > > The US convention (AAA)BBB-CCCC is not just evolving into  
> > > AAA-BBB-CCCC;  
> > > now I'm seeing more and more of the "international" style:  
> > > AAA.BBB.CCCC  
> > > . This appears in some "chic" guidebooks.  
> >  
> > I tried using that format, until I pulled a text file into  
> > Excel and it  
> > changed all the phone numbers into "real numbers" and  
> > deleted terminal  
> > zeros. Excel also has this annoying habit with IP  
> > addresses, changing  
> > 10.0.0.10 to 10.0.0.1. I can't find a way, in the \*import\*  
> > function, to  
> > define these numbers as "text" so that Excel will leave them  
> > alone upon  
> > import. Sigh.  
>  
> I suspect that you may be using an old version of Excel.  
>  
> I have just tested this using Excel 2000 (version 9.0.3821 SR-  
> 1).  
> If I open a text file containing your example, the Text Import  
> Wizard  
> appears. I accept its first two default suggestions (it  
> correctly  
> deduced how I had delimited fields within the file), then it

gives  
> me a choice of General, Text, Date (with six sub-choices), or  
Skip,  
> for each field; I then select Text for the field in question.  
>  
> There is an alternative way to do this which may work for older  
> versions of Excel. If you open a new spreadsheet, select the  
> appropriate column(s), then Format Cells Text, you can copy  
data  
> from a text file (e.g. from within Notepad) and paste it into  
the  
> cells you have already formatted. This works because Excel  
tries  
> to deduce the format of General cells but not Text cells.  
>  
> Mark  
>  
> p.s. For completeness, I have just imported the same test file  
and  
> accepted all of the Text Import Wizard's defaults. It  
correctly  
> deduced that IP addresses should be left alone (i.e. formats  
them  
> as text rather than numbers, even though the Format Cells  
dialogue  
> shows that they have General format rather than Text).  
> --  
> Mark Lomas <mark.lomas@tmalomas.com>  
>  
>  
> From neil.maller@gte.net Mon Nov 12 08:26:52 2001  
> Date: Mon, 12 Nov 2001 08:26:53 -0500  
> Subject: Re: Excel and non-decimal dots  
> From: Neil Maller <neil.maller@gte.net>  
> To: <msb@vex.net>  
>  
> on 11/11/01 9:52 PM, RISKS List Owner at risiko@csl.sri.com  
wrote:  
>  
> > Date: Wed, 7 Nov 2001 13:43:25 -0500 (EST)  
> > From: msb@vex.net (Mark Brader)  
> > Subject: Excel and non-decimal dots  
> >

> > \* From: magical@rahul.net  
> > \* Newsgroups: alt.usage.english  
> > \* Subject: Re: Telephone Area Code  
> > \* Message-ID: <7bqiutgjqqgl1tu29qd6ak615c14pbcfavo@4ax.com>  
> > \* Date: Wed, 07 Nov 2001 17:07:08 GMT  
> >  
> > On Wed, 07 Nov 2001 07:54:15 GMT, in alt.usage.english, David  
> > Hecht <davidhecht@prodigy.net> created  
> >  
> >> The US convention (AAA)BBB-CCCC is not just evolving into  
> >> AAA-BBB-CCCC;  
> >> now I'm seeing more and more of the "international" style:  
> >> AAA.BBB.CCCC  
> >> . This appears in some "chic" guidebooks.  
> >  
> > I tried using that format, until I pulled a text file into  
> > Excel and it  
> > changed all the phone numbers into "real numbers" and  
> > deleted terminal  
> > zeros. Excel also has this annoying habit with IP  
> > addresses, changing  
> > 10.0.0.10 to 10.0.0.1. I can't find a way, in the \*import\*  
> > function, to  
> > define these numbers as "text" so that Excel will leave them  
> > alone upon  
> > import. Sigh.  
> >  
> > Mark,  
> >  
> > You're probably already aware of this, but preceding your  
> > would-be text in  
> > Excel by a single <'> character (apostrophe) will define it as  
> > text and  
> > suppress any reformatting. This apostrophe will not be  
> > displayed in Excel,  
> > although it'll still be there if you export the cell contents.  
> >  
> > It may not be possible to insert the extra character as part  
> > of Excel's  
> > import process, but I'm sure you can figure out a way to  
> > prepend the  
> > apostrophe beforehand. For instance this would be easy in MS  
> > Word using the

> Replace function.  
>  
> We use Excel extensively to compose tables for technical  
manuals, so face  
> its auto formatting quirks on a daily basis. RISKS of using a  
spreadsheet  
> program for non-mathematical tasks...  
>  
> Regards,  
>  
> Neil

> From mchinni@pica.army.mil Wed Nov 14 11:42:55 2001  
> From: "Chinni, Michael J [AMSTA-AR-CI]" <mchinni@pica.army.mil>  
> To: "'msb@vex.net'" <msb@vex.net>  
> Subject: Re: [Risks Digest 21.74](#)  
> Date: Wed, 14 Nov 2001 11:43:08 -0500  
>  
> Mark,  
>  
> Regarding your item in the [Risks Digest 21.74](#) (see below),  
when  
> importing a text file into Excel (i.e. opening a text file  
from within  
> Excel) there's a step where you can define the data types for  
each column  
> (in Excel 2000, it's step 3 of 3 in the Text Import Wizard).  
In that step  
> just change the data type for the columns you want left alone  
to "Text" (the  
> default is General).  
>  
> ...Mike Chinni

---

## ✶ Porn spam being sent in my name

Nickee Sanders <njs@ihug.co.nz>  
*Tue, 13 Nov 2001 12:01:13 +1300*

I maintain a mail account at deja.com (continued by google), as spam protection for my real e-mail account. Every now and then I log on and delete the accumulated spam.

I logged on the other day and found a bounce notification message. I was surprised at this and opened it. Imagine my surprise to find that the original (bounced) message had been spam, apparently sent from me!

It seems that someone had somehow picked my e-mail address to use in forging their e-mail header. Worse yet, the spam was porn spam.

How much worse can things get? Up till now, I at least had the comfort that unsolicited e-mail (spam, viruses, etc) was in my control, and that with a little care I could protect myself from most of it. Now, I don't even have that.

---

## **⚡ Re: Kids' learning game site becomes porn site (Smith, [RISKS-21.74](#))**

Dan Fandrich <dan@coneharvesters.com>

*Wed, 14 Nov 2001 00:10:38 -0800*

It's refreshing to see that Ernst and Young actually cared enough about the problem to do something about it. Back in May, the same pornographers bought up close to 2000 expired domains (that I could tell), including

domains owned by respectable organizations with hundreds of inbound links, such as the TCL Consortium, XIII International AIDS Conference, Evian, Universal ADSL Working Group, and Craig's List. I tracked down the original owners of about 60 of these sites with the most inbound links and warned them of the problem (this wasn't entirely altruistic as I was operating a service at [www.moveannouncer.com](http://www.moveannouncer.com) that could help them bypass the worst effects the problem).

Five months later, only three of those 60 sites have done anything about their former domains, either buying them back from the extortioners or getting links changed to their new sites. Some of the former owners I talked to seem to have trouble seeing that their web sites did not stand in isolation, that people outside their organization had links to their web site and others had bookmarks and those links attached to their names were now serving up porn. I got responses to the effect of "We have a new domain name now, so we don't care what happens to the old one."

One certainly takes a RISK in letting one's domain name expire, but when the gamble fails and what must be about the worst case scenario occurs, the indifference I've seen surprised me. I find it hard to believe that so many people have so little respect for their viewers and customers.

## **✶ Re: Kids' learning game site becomes porn site (Smith, [RISKS-21.74](#))**

Malcolm Pack <risks3@potnoodle.net>  
Tue, 13 Nov 2001 10:44:55 +0000

YaBB, a popular PERL web-based forum application, recently moved to  
<<http://yabb.xnull.com/>> from <www<dot>yabb<dot>org>, which is  
now  
pure pr0n. I've munged the link. Anyone is welcome to unmung it,  
of  
course. <puerile snigger>

<<http://yabb.xnull.com/community/?board=general&action=display&num=1000638654>>

says it all. Also it implies that the presence of pr0n on the  
"hijacked" site is a blackmail tool, which would explain why so  
many  
domain names obviously targeted at children become (apparently  
inexplicably) pr0n sites.

I'd never thought of pr0n as a weapon. Perhaps the new US  
PATRIOT Act  
<<http://www.zdnet.co.uk/itweek/columns/2001/42/bingley.html>>,  
ridiculous though it may be, could be diverted against these  
amoral  
cybersquatters for a while before it gets repealed.

---

## **✶ Computers & bureaucracy help spread of foot & mouth disease**

"Charles Shapiro" <cshapiro@numethods.com>  
Thu, 15 Nov 2001 08:52:51 -0500

According to an editorial in the \*London Daily Telegraph\*, a  
combination of

cumbersome bureaucratic systems and inaccurate map databases is to blame for the rapid spread of hoof & mouth disease in Britain. The essay details one incident of overreliance on poor quality data which led to a substantial loss to a shepherd's flock. It also blames delays and foolish acts on centralized decision making.

Risk: Look out at the Big Room from your monitor once in a while.

<http://www.dailytelegraph.co.uk/dt?ac=006527651614093&rtmo=a5d9qChJ&atmo=rrrrrrrrq&pg=/01/11/12/do01.html>

Charles Shapiro <charles.shapiro@numethods.com>

[See also previous Foot-and-mouth virus propagation items, PGN, [RISKS-21.31](#) and Ursula Martin, [RISKS-21.33](#). PGN]

---

## ⚡ Re: Another SRI-wide power outage (Rowland, [RISKS-21.74](#))

Kelly Bert Manning <bo774@freenet.carleton.ca>  
*Wed, 14 Nov 2001 00:31:10 -0500 (EST)*

Back in the days of SNA I could tell when the Xerox tech was in to work on the Xerox in the basement because both IBM cluster controllers would fail simultaneously. They were about a meter away with their Gandalf modems on top. The Xerox tech would decide that the the pair of side by side tops of the controllers made an excellent surface for him to flop his huge folder of tech charts onto, toggling the power switches on both modems off.

Power failures were sometimes an event to take advantage of. Our first IBM terminals were installed about the time that our corporate president decided that we could convert our largely Honeywell based applications from GCOS 4JS et al to to MVS for about \$1 million and in less than a year (turned out to be not quite done 2 years and \$10 million later, but that is another risk). We were a bit surprised to see the terminals turned on but blank and not responsive, for most of a week, until the power failed for longer than the motor generator flywheel could smooth out. The HIS terminals were in use within a few minutes of power being restored, but about 25 minutes later the MVS terminals all started showing netsol logos for the first time. We got a phone call shortly after asking us to confirm that. Apparently SNA at the time didn't recognize new terminals until the next IPL, giving rise to the short lived line about "if IBM designed the phone system...". Life is much more flexible with TN3270 these days.

---

## 🔥 REVIEW: "White Hat Security Arsenal", Aviel D. Rubin

Rob Slade <rslade@sprint.ca>

*Mon, 19 Nov 2001 08:04:40 -0800*

BKWHTHSA.RVW 20010814

"White Hat Security Arsenal", Aviel D. Rubin, 2001, 0-201-71114-1,

U\$44.99/C\$67.50

%A Aviel D. Rubin rubin@research.att.com

%C P.O. Box 520, 26 Prince Andrew Place, Don Mills, Ontario  
M3C 2T8  
%D 2001  
%G 0-201-71114-1  
%I Addison-Wesley Publishing Co.  
%O U\$44.99/C\$67.50 416-447-5101 fax: 416-443-0948 bkexpress@aw.  
com  
%P 330 p.  
%T "White Hat Security Arsenal: Tackling the Threats"

The distinctive of this book is that it approaches security as a series of specific problems or concerns. The non-distinctive, if you will, is that it attempts to address all audience levels; users, IT professionals, academics, and administrators. A series of icons identifies, at the beginning of each chapter and at particular sections of the text, who should read the various segments of the text.

Part one examines the size and scope of the security issue. Chapter one starts out with perhaps our biggest problem, as security people: the insistence on secrecy by companies who get hit, and the fact that this obstinate refusal to discuss the facts makes our job, in protecting institutions, that much harder. A brief look at what may be at risk from security problems is given in chapter two. Recent e-mail viruses are reviewed in chapter three, but they get an interesting treatment. The material, while technically sound, concentrates on the general security attitudes and lessons to be learned, as they apply to computer use in general.

Part two looks at information storage. Chapter four's problem

is to ensure that information is kept private if an attacker gets hold of your machine, and Rubin gives a good introduction to symmetric encryption and provides tips on passwords. If you are concerned about storage at remote sites over an insecure network, chapter five touches on passwords again, and asymmetric encryption. Chapter six is supposed to deal with securing backups, but seems to get a bit confused, although it does provide some good tips, as well as an overview of some online backup services.

Part three considers the problems of data transfers over an insecure net. Chapter seven introduces authentication and some of the problems of public key management. Session keys and key exchange are examined in chapter eight: it has an academic icon at the top of the chapter, and non-specialist users might get a bit confused here. The aspects of virtual private networks are reviewed in chapter nine, and the book begins moving towards the usual technology oriented model.

Part four looks at network threats. Chapter ten explains firewalls while eleven discusses a variety of network based attacks.

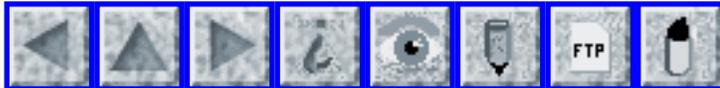
Part five doesn't really have a central theme. The title of chapter twelve is "Protecting E-Commerce Transactions," but most of the text deals with the Secure Sockets Layer for Web browsers. Privacy, in e-mail and Web browsing, is discussed in chapter thirteen, but many areas are left unexplored.

For managers and users who are not specialists in computer and

communications security, this book provides a readable and accurate introduction to a number of important topics. There are, unfortunately, a number of gaps in terms of the total security picture, but that is probably to be expected when taking the problem oriented approach. Rubin does not talk down to the audience and does not oversimplify, and this work therefore is superior to a number of the introductory books on the market.

copyright Robert M. Slade, 2001    BKWHTHSA.RVW    20010814  
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 21: Issue 77

Weds 21 November 2001

## Contents

- [FBI targets suspects' PCs with spy virus](#)  
[NewsScan](#)
- [A tell-all that ZD would rather ignore](#)  
[Declan McCullagh via Monty Solomon](#)
- [Risks with automated counting of ballot papers: Australia](#)  
[Chris Maltby](#)
- [Evolution, Thermodynamics, and Software Bugs](#)  
[William Colburn](#)
- [Re: Programming error scrambles election results](#)  
[Paul Terwilliger](#)  
[Ralph Barone](#)  
[Richard Stein](#)  
[Edward Reid](#)  
[Bob Dubery](#)
- [Re: Researchers probe Net's 'dark address space'](#)  
[Scott Peterson](#)
- [Fun with automated car washes, or the importance of interface design](#)  
[Aaron M. Ucko](#)
- [Re: Feds make record counterfeit software seizure](#)  
[Denis Haskin](#)

- [Re: Glitch in iTunes Deletes Drives](#)  
[Paul Ward](#)  
[Geyser Admin](#)
  - [Re: Sweden's public radio reportedly bans SETI...](#)  
[Nick Brown](#)
  - [Re: Telephone Area Code](#)  
[Patrick O'Beirne](#)
  - [Re: Google freely giving out ...](#)  
[Rebecca Wright](#)
  - [Re: DoS attack on Mac OS9](#)  
[David Cake](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

## ✶ FBI targets suspects' PCs with spy virus

"NewsScan" <newsscan@newsscan.com>

Wed, 21 Nov 2001 07:32:53 -0700

The FBI is working on software that could insert a computer virus into a suspect's computer capable of reading encrypted data. The software, known as "Magic Lantern," installs "keylogging" software that can capture keystrokes typed on a computer. The virus can be sent via e-mail. Once on the targeted PC, it waits for a suspect to launch the Pretty Good Privacy encryption program and then logs the passphrase used to start the program, essentially giving agents access to the keys needed to decrypt files. The Magic Lantern software is part of the FBI's "Enhanced Carnivore Project Plan," which operates under the umbrella project name of Cyber Knight. Electronic Privacy Information Center attorney David Sobel says

privacy

issues arise when keylogging results in "overly broad" searches, since it would be possible to observe every keystroke typed by the suspect, even if a court order specified only encryption keys. The FBI has already used a less-sophisticated version of the software to build the high-profile racketeering case against Nicodemo Scarfo, but had to manually turn the system on and off in order to comply with the court order.

[MSNBC/Wall

Street Journal 21 Nov 2001; NewsScan Daily, 21 November 2001]

<http://interactive.wsj.com/articles/SB10062942834030720.htm>

(sub req'd)

[Insertion by e-mail probably works well for Microsoft software, which is

prone to that kind of attack. Various reports suggest that Magic Lantern

can also plant itself by penetrating systems. Penetrability of supposedly

secure systems has long been noted here, with further risks resulting from

a weak system that is directly networked to supposedly more secure systems

(especially if done with single-sign-on authentication). This may not be

a case where one good (LAN-)turn deserves another. PGN]

---

## **✶ A tell-all that ZD would rather ignore**

Monty Solomon <monty@roscom.com>

*Tue, 20 Nov 2001 08:39:52 -0500*

Declan McCullagh, Wired News, 20 Nov 2001

If you subscribe to any of Ziff-Davis' computer magazines, you may want to double-check your credit-card bill next month. Ziff-Davis Media, which publishes such popular tech titles such as Yahoo Internet Life and PC Magazine, accidentally posted the personal information of about 12,500 magazine subscribers on its website. On 19 Nov 2001, ZD removed the data, which included hundreds of credit-card numbers, and said its engineers had taken steps to prevent additional security leaks.

<http://www.wired.com/news/ebiz/0,1272,48525,00.html>

---

## ⚡ Risks with automated counting of ballot papers: Australia

Chris Maltby <chris@sw.oz.au>  
*Tue, 20 Nov 2001 16:00:10 +1100*

As RISKS readers may be aware there was a national election in Australia on 10 Nov 2001. Australian electoral procedures have many features which US readers in particular would find unusual, but perhaps the most surprising of all is the method used to elect Senators for each of the states.

A preferential voting system is used (a complete order of preference must be shown) and those candidates who receive a quota (a proportion based on the number of positions to be filled) are elected. Any votes surplus to quotas are redistributed at reduced value, and least preferred candidates are excluded until all positions are filled. The interested can refer to

<http://www.aec.gov.au/pubs/factfiles/factsheet7.htm> or the truly masochistic

to the legislation which specifies the counting method.

<http://scaleplus.law.gov.au/html/pasteact/0/57/0/PA003450.htm>

In a normal half-senate election, 6 senators are elected, meaning that a the quota value is about 14.3% -- within the bounds of possibility for smaller parties.

With a trend toward an increased number of candidates, a simplification was introduced in the late 1980s whereby political parties could nominate a preference "ticket" and the voter can choose the party ticket by voting in boxes above a thick line which divides the ballot paper. Alternatively the voter can number all the squares below the line (65 in all in the recent election in New South Wales). Since its introduction, the number of voters using the above the line method has grown at each election and was above 95% in 2001.

The increase in ticket voting has made feasible the automated "scrutiny" or determination of the result, and the Electoral Act was amended before the 1998 election to permit this. All that is needed is for the 3-5% of below the line papers to have their order of preference captured, the total number of voters who selected each of the tickets and then the legislated method can be applied and the result determined "instantly" instead of taking several weeks by the manual method. The taxpayer wins if the time taken to input the ballots is shorter than the time taken by the manual procedure...

But the risk is in the accountability. In a manual election, each of the candidates is entitled to appoint an observer (scrutineer) who may check for irregularities in the process. It may be mind numbingly boring, but it is feasible.

The automatic system is much more difficult. The legislation permits the scrutineer access only to a record of:

- \* the preferences on the ballot-papers ... stored in the computer; and
- \* the ballot-papers that ... are transferred at each count; and
- \* the progress of the count of the votes, at each count.

Note that the source code of the software which determines the result nor its operating environment are explicitly not available for scrutiny, meaning that each scrutineer must be able to reproduce the process independently to sufficient accuracy to detect errors or fraud (refer to the legislation link above). Also the scrutineer(s) must attempt to observe the accuracy of hundreds of data entry staff as they enter the ballots at full speed.

As the result can be affected by cascading differences triggered by tiny numbers of votes changing the order of exclusions, it's probably only a matter of time before there is a very interesting case in the Court of Disputed Returns.

---

## **✶ Evolution, Thermodynamics, and Software Bugs**

"Schlake ( William Colburn )" <schlake@nmt.edu>

Mon, 19 Nov 2001 13:25:00 -0700

(Re: Programming error scrambles election results ([RISKS-21.74](#)))

There is an interesting paper I recently read. It shows that biological evolution is just like debugging. Selective pressure, such as poison (debugging), on a biological system will kill as few members as possible to keep the system stable. Software bugs are the same way. Debugging is a selective pressure (selected by the debugger to meet their expectations) and will remove as few software bugs as possible.

See "Murphy's law, the fitness of evolving species, and the limits of software reliability", at:

<http://www.ftp.cl.cam.ac.uk/ftp/users/rja14/babtr.pdf>

The authors webpage is at:

<http://www.cl.cam.ac.uk/~rja14/>

---

## **⚡ Re: Programming error scrambles election results ([RISKS-21.75](#))**

Paul Terwilliger <pault@gsinet.net>

Mon, 19 Nov 2001 15:56:13 -0500

Both Mr. Marson and Mr. Kos, in their comments about the San Bernardino election problem, make a common mistake.

There is programming, and there is programming.

"Programming" an election is not writing software. It is akin to

programming a VCR. In other words, entering data to describe the layout of the ballot. Sometimes vendors do this, sometimes county employees do.

(Even though I do not know which particular vendor's equipment was used, all are alike in this regard.)

Does this make testing unnecessary? Of course not. But let's make sure we understand where the failure was.

Paul Terwilliger, Sequoia Voting Systems, Inc.

---

## **[Re: Programming error scrambles election results \(Marson, RISKS-21.74\)](#)**

"Barone, Ralph" <Ralph.Barone@BCHydro.bc.ca>

*Mon, 19 Nov 2001 14:08:47 -0800*

I believe that in order to truly test a piece of software, at least two testers are needed. The first would be somebody with a complete enough understanding of the problem that he/she could have coded the program themselves. This person would review the code for logical errors, robustness of algorithms, etc... The second tester would be a person with minimal knowledge of the system (representative of the least trained person ever likely to operate the system). This person will unwittingly test all the user interface and data checking assumptions made by the original programmer.

---

## **✶ Re: Programming error scrambles election results (Marson, [RISKS-21.74](#))**

Richard Stein <rstein@sgi.com>

*Mon, 19 Nov 2001 16:13:00 -0800*

If you want to know the cost of quality, prepare to purchase it!

A 'real' software test engineer, one who is exceptionally knowledgeable of the fundamental technology mechanisms residing at the core of modern products (like threads, synchronization, scheduling, signals, process tracing, message passing, VM, etc.) is mighty, mighty rare and plenty expensive.

Certain cultural and educational barriers forestall the creation of many.

Peer ostracism, managerial indifference, and professional lassitude often conspire against this career choice.

The best folks prefer product engineering (aka 'development'). Hell, a good test engineer must continuously author and develop test assets well ahead of any product engineering activity. In the past 7 years, I have authored in excess of 400K statements of PERL/C/C++ comprising thousands of individual functional test assets and dozens of reliability evaluations. I know kernel hacks who have struggled for months to find a 1 line race condition fix arising from a wimpy program.

Creating non-deterministic product evaluations that compel races, corrupt data, generate deadlock, cause resource leakage, panic, coredump, or other fatal conditions is more of an art than a method. No matter how stupid or non-sensical an input, a product must remain deterministic and self-consistent (this is the famous user-is-an-idiot postulate).

Deterministic evaluations consume substantial test engineering cycles: all those inputs, a little product logic, and assertions of output takes many keystrokes. Such exhaustive measurement is often the only means to show program feature and function correctness. What I'd give to out-think Alan Turing on this issue!

Many for-profit organizations do not really understand that test engineers author intellectual property too: IP the customer does not purchase, but what they experience as a consequence of test asset quality ; If the test assets stink, the product stinks.

That's what test engineers do -- function as editors (as in newspaper publications) to raise product IP quality. To be successful, test engineers must embody the worst customers in the world, and the best friend a product can have. The only acceptable customer feedback is a purchase, not a complaint.

How does proactive test engineering compare to a 'nuclear' customer support hotline post-release? Its hard to query corpses -- especially dot-bombs. If management believes any warm body will suffice to

successfully and  
thoroughly evaluate 1Mline+ C++ software toxic wastedumps, dig  
up a corpse  
from a cemetery and apply a space-heater, but don't hire a  
button pusher.

We all know its far cheaper to fix bugs in the system before  
release, and  
even easier/cheaper when in the earliest SDLC phases. But  
testing and other  
means to ensure quality are often short-changed because of  
disciplinary  
failure and organizational, ethical lapses -- covert  
institutionalized  
violence.

Richard M. Stein, StudioCentral Test Engineering Contractor 650-  
933-7391

---

## ✶ Re: Programming error scrambles election results ([RISKS-21.75](#))

Edward Reid <edward@paleo.org>  
*Tue, 20 Nov 2001 10:50:03 -0500*

Takes a lot more than understanding the problem, etc.. The  
person who really  
understands the problem is generally only going to enter  
expected, correct  
data for the problem domain. The programmer tends to be limited  
by the  
expectations of the program, the skilled user by the  
expectations of the  
problem domain. Good testing is a different skill. If you want a  
program to  
be ready for prime time, get it tested by someone skilled in  
testing. Of  
course the tester must know something about the problem domain,  
and testing

by both the programmer and the skilled user are valuable too.  
But testing  
is a skill in itself.

---

## **✶ Re: Programming error scrambles election results (Kos, [RISKS-21.75](#))**

"Bob Dubery" <bdubery@netcare.co.za>

*Tue, 20 Nov 2001 07:37:47 +0200*

> nobody (not even I! ;) can be relied on to find their own bugs.

And also there is less chance of them LEARNING from their bugs -  
so the  
"method" behind the bug tends to propagate.

I had been arguing about the existence of a bug with two  
programmers from  
another dept in the IT organisation that I work for.

Eventually I got to take a peek at the code in which - according  
to me - the  
bug had to exist. I found it in minutes. The programmer  
concerned had  
written code that ignored a lock in the database with the result  
that  
updates were sometimes "lost" if two instances of the code were  
running  
simultaneously.

When I showed the programmer (a junior person) who wrote the  
code the bug  
and explained it she quickly grasped the flaw in her logic and  
went off to  
check several other bits of work she'd done to see if she had  
reproduced the  
bug. She now also understands a particular aspect of her job and  
the

language she works with better than she used to.

A test in a multi-user scenario and/or a code review would have quickly uncovered a bug that caused some acrimony and a loss of money - and would have resulted in a programmer who had had improved their craft.

One of the RISKS of not having code reviews and good test procedures in place is that inexperienced junior programmers will become poorly experienced senior programmers and the bugs will propagate.

---

## **✶ Re: Researchers probe Net's 'dark address space' (Poulsen, R-21.75)**

Scott Peterson <scottp4@mindspring.com>  
*Mon, 19 Nov 2001 14:29:19 -0800*

I'd suggest that a large part of this is due to explicit blocking of IP ranges by system administrators. This could either be local blocks or published lists like MAPS or SPEWS. Getting on SPEWS, for example will make about 30% of the Internet unreachable if you get listed.

Also, for cable modems, I'd think a large part of this is the arrogance, unresponsiveness and incompetence of the administrators of the cable networks, especially @home. They've gotten into lots of local block lists because they won't shut off abusers or even respond to complaints.

## ✈ Fun with automated car washes, or the importance of interface design

"Aaron M. Ucko" <amu@alum.mit.edu>

19 Nov 2001 21:53:57 -0500

My wife and I had an unexpected adventure when we went to get our car washed at a gas station the other day. (I am withholding the name of the chain to protect the not-so-innocent, and because it is probably not the only culprit anyway.)

First, some background: the system is fully automated, and offers three levels of operation. (The cheapest doesn't even dry the car, and the most expensive includes tire scrubbing and other frills.) Because we had recently gotten the car used, we decided to go for "The Works." Also, the station offers a discount with the purchase of 8 gallons or more of gas; in order to get this discount, you need to buy a code for the machine with your gas.

Anyway, the first problem we encountered came about when ordering: the display at the pump told us to press 1, 2, or 3 to select a cycle, but did not specify which was which. Assuming that it went from cheapest to most expensive, we pressed 3, only to be told that we had selected the basic cycle. Fortunately, it asked for confirmation, so we went back and selected 1 instead.

Next, we drove up to the car wash (which involved waiting in

line for a little while, waited for the previous driver to finish, punched in our code (for "The Works"), and drove into the machine. It started to wash our car, but then stopped in the middle of the cycle -- with a little barrier effectively preventing us from driving out the other side. (We could probably have driven over it if we had pressed hard enough on the gas, but it didn't seem like a great idea.) The machine appeared to be completely dead; the screen which normally displays something like "enter," "exit," or "washing" was blank.

Experimentally, we backed up slightly, at which point the machine told us to drive forward again; when we were back in the target position, it started all over -- with a basic cycle, which it at least finished properly. At that point, we drove out unhindered and went to complain to the management. We convinced them to give us a new code for "The Works", and returned to the back of the car-wash line.

When we got back inside the machine, it stopped at the same point as before. This time, we just gave up and waited for something to happen; after a few minutes, the attendant came out (at the behest of the driver behind us), and motioned that we should again drive backwards for a moment and then back forwards to the target position. This maneuver again caused the machine to restart -- this time with what appeared to be a "deluxe" cycle. Since that cycle included the remainder of the things we wanted, we decided that it was

good enough and that we had wasted enough time there, and so simply drove off.

Our hypothesis is that both times, the drivers behind us had confused the machine by entering their codes before we were done -- an action which the interface allows, and even appears to encourage[1] -- and that each time we backed up, it restarted with the cycle the next driver had ordered.

The risks?

- \* Poorly presented menus can lead to undesired selections.
- \* Badly designed machines can trap their users. (Note that in this case, a Big Red Button would not have sufficed, since it was not entirely clear that the machine might not suddenly restart and injure whoever got out of the car to push it.)
- \* Systems that prompt for input before they are ready for it can fail unpleasantly.

[1] After telling one driver to enter, it immediately prompts for another code.

Aaron M. Ucko, KB1CJC <amu@mit.edu> (finger amu@monk.mit.edu)

[Nonatomic transactions can be quite explosive. PGN]

---

## ⚡ Re: Feds make record counterfeit software seizure ([RISKS-21.75](#))

Denis Haskin <Denis@HaskinFerguson.net>  
Mon, 19 Nov 2001 17:24:49 -0500

Um, perhaps I'm being naive, but it's not clear to me what the "risks to the public in computers and related systems" is in this case. Sure, there's a risk that consumers may be buying software that's not legit, but is there an allegation that the software is flawed in some way? Isn't this sort of like buying a Rolex on a NY street corner?

---

**⚡ Re: Glitch in iTunes Deletes Drives (Solomon, [RISKS-21.74](#))**

<pasward@styx.uwaterloo.ca>  
*12 Nov 2001 12:20:39 -0500*

NO! The problem was NOT that some "bleary-eyed coder" missed a couple of quotes. The problem was that Apple's process for reviewing software prior to shipping to catch the inevitable syntactically correct but semantically flawed code was broken. And broken badly if such a obvious error could slide through undetected.

paulward (DrGS)

---

**⚡ Re: Glitch in iTunes Deletes Drives ([RISKS-21.74](#))**

Geyser News Server Admin <news-admin@geysers.org>  
*Mon, 12 Nov 2001 11:39:04 -0800*

Before the Mac haters out there take any glee from this

incident, a  
clarification is important.

What was left out was the reason why the quotes are important--  
On the Mac,  
file and directory and disk names can and do contain spaces.  
With the new  
Unix-based OSX, long-time mac users are discovering the hard way  
that spaces  
are used as delimiters in scripts and in parsing, so filenames  
containing  
spaces can have unintended results. Most Unix code samples and  
docs assume  
that no one ever puts spaces in their file names, so the samples  
never show  
quotes being used, and some docs don't mention this need either.

Just about every programmer making the Mac switch from OS 9 to  
10 finds  
this out the hard way, just not as publicly and catastrophically.

The risk-- changing the underlying behavior of familiar  
software, and  
not being aware of all the assumptions behind that underlying  
behavior.

---

## **⚡ Re: Sweden's public radio reportedly bans SETI... ([RISKS-21.74](#))**

BROWN Nick <Nick.BROWN@coe.int>  
*Mon, 12 Nov 2001 09:15:43 +0100*

I agree that it's unlikely that the US military needs extra  
Swedish PC  
computing power to plot missile trajectories, but the Swedes  
have been here  
before. In the mid-90s the Swedish parliament and other  
government offices  
acquired Lotus Notes, and one factor in their choice was the

"secure"

encryption it provided. Until they found out that the CIA had a master key.

So the line between "conspiracy theory" and "justifiable paranoia" is perhaps blurred in this case.

There is also the RISK that in running any code from SETI@home, you are trusting SETI's site not to be hackable by someone who might want to run some other code on your computer. If someone put a replacement client in there which trashed your hard disk at a given date/time, I suspect the worldwide damage would put the "ILoveYou" worm to shame.

---

## ✉ Re: Telephone Area Code (Hecht, [RISKS-21.74](#))

"Patrick O'Beirne" <pobeirne@sysmod.com>

*Mon, 12 Nov 2001 09:16:35 +0000*

> I can't find a way, in the \*import\* function, to define these numbers as

> "text" so that Excel will leave them alone upon import. Sigh.

Text Import Wizard step 1 - choose fixed/delimited

Step 2 - column breaks

Step 3 is where you set the column format - choose Text for IP addresses

<http://www.sysmod.com/spreads.htm>

Patrick O'Beirne B.Sc. M.A. FICS

---

## ✉ Re: Google freely giving out ... (Re: Ziglar, [RISKS-21.75](#))

Rebecca Wright <rwright@research.att.com>

*Tue, 20 Nov 2001 17:37:45 -0500 (EST)*

Listings can (at least now) be removed using a form found at <http://www.google.com/help/pbremoval.html>, which was linked to from the "More phonebook listings" on my Google telephone listing. This form itself is not without risks. First, they require (off-line) authentication only for removal of business sites, so individuals can have their listings removed by others even if they would prefer to have their listings remain. Second, your communication with Google about your phone listing can actually help them establish its correctness (and they ask for your e-mail address too), so depending on your trust level in Google to handle your personal information, you might consider it better to remain silent than to voluntarily give them verified information about yourself.

[RISKS received a Google-plex of e-mail on this subject. This information is widely available on the Internet, on CD-ROM, etc. Thanks to all who responded. PGN]

---

## **★ Re: DoS attack on Mac OS9 (Gat, [RISKS-21.73](#))**

David Cake <dave@difference.com.au>

*Mon, 12 Nov 2001 13:31:52 +0800*

>Sure, you can change passwords if you have physical access to the machine.

>You can also boot any Mac with a MacOS 9 CD and completely circumvent all >protection.

Firmware security can make it much more difficult to boot from a MacOS 9 CD (or any other bootable CD), and avoids some similar simple methods of circumventing password authentication (booting in single user mode). Firmware security is a recent, and poorly documented, addition to the Macintosh that is not present on all models, and on many machines will require a firmware update. It is a significant protection against the casual, Macintosh capable but not truly expert, attacker, and is thus probably a good idea for situations such as unattended kiosks or laboratory machines. It cannot, however, be completely relied on.

There are two methods to bypass firmware security. One is a reasonable and prudent method - if you change the RAM in the machine, it also resets the firmware security. Perhaps there will be unintended consequences from those are unaware of this poorly documented side effect, but it is necessary that there be some means of disabling the feature to prevent machines being rendered unbootable, and it is appropriate that it be some feature that requires access to the internals of the machine for a reasonable amount of time. If you are in a situation where firmware security is an issue, you should also be implementing physical security (Apple generally makes it easy to secure access to the case with a padlock or similar on most models).

Unfortunately, there exists a weakness in the implementation of

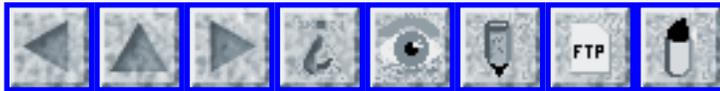
the firmware security that enables the dedicated attacker to discover the Open Firmware password and thus bypass this protection, and a program to exploit this vulnerability is available.

<http://www.securemac.com/openfirmwarepasswordprotection.php>

Luckily, it runs only under Mac OS 9, so Mac OS X machines are relatively safe (it does not run under Classic), but this cannot be relied upon, as the same underlying vulnerability exists and it is simply a matter of someone writing code to exploit it.

Apple does appear to be gradually increasing the amount of security, and definitely appear to be treating security on Mac OS X as a serious issue. Unfortunately, there are still some weaknesses that have been discovered.

David Cake (Macintosh and Unix consultant), Difference Engineering



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 21: Issue 78**

**Thursday 22 November 2001**

## Contents

- [Playboy says hacker stole customer info](#)  
[Monty Solomon](#)
- [Euro changeover risk](#)  
[Carl Fink](#)
- [The cure is only slightly worse than the disease...](#)  
[Russell Stewart](#)
- [My daughter is failing high school!](#)  
[Jeremy Epstein](#)
- [Network Solutions ad inadvertently names my domain](#)  
[Fredric L. Rice](#)
- [Another date risk](#)  
[Leonard Erickson](#)
- [Re: Researchers probe Net's 'dark address space'](#)  
[Arthur Smith](#)
- [Glitch in iTunes Deletes Drives](#)  
[Dave Katz](#)
- [Re: FBI targets suspects' PCs with spy virus](#)  
[R.S. Heuman](#)  
[Rob Slade](#)
- [RISKS-21.77 was rejected by some filters](#)

[PGN](#)

- [Re: Porn spam being sent in my name](#)  
[Andrew Klossner](#)
  - [Re: Programming error ...](#)  
[David Gillett](#)
  - [Re: Toaster failures](#)  
[Marcus Didius Falco](#)
  - [The more things change](#)  
[Mike Albaugh](#)
  - [Re: IP: 800 directory "assistance" redirecting calls](#)  
[Rob Bailey](#)  
[Clay Jackson](#)
  - [Re: National ID cards](#)  
[Henry Baker](#)
  - [Re: Windows XP accounts by default are administrator with no password](#)  
[Mark Wilkins](#)
  - [Let's get really paranoid about e-mail and spam...](#)  
[Allan Hurst](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

## ✶ **Playboy says hacker stole customer info**

Monty Solomon <monty@roscom.com>

*Tue, 20 Nov 2001 23:01:48 -0500*

By Greg Sandoval and Robert Lemos, CNET News.com, 20 Nov 2001

Playboy.com has alerted customers that an intruder broke into its Web site and obtained some customer information, including credit card numbers. The online unit of the nearly 50-year-old men's magazine said in an e-mail to customers that it believed a hacker accessed "a portion" of Playboy.com's computer systems. In the e-mail, a copy of which was reviewed by

CNET

News.com, Playboy.com President Larry Lux did not disclose how many customers might have been affected.

Playboy.com encouraged customers to contact their credit card companies to check for unauthorized charges. New York-based Playboy.com also said it reported the incident to law enforcement officials and hired a security expert to audit its computer systems and analyze the incident. [...]

<http://news.cnet.com/news/0-1007-200-7932825.html>

---

## ✶ Euro changeover risk

Carl Fink <carlf@dm.net>

Wed, 21 Nov 2001 13:03:46 -0500

An Irish emigrant to Spain had an unexpected windfall when his Dublin bank

accidentally credited more than 300,000 euros (\$264,800) -- instead of

300,000 pesetas -- to his new account, newspapers reported on Wednesday.

(Reuters, <http://news.excite.com/news/r/011121/07/odd-ireland-dc>)

Surely European banking software has always had to handle currency conversions?

Carl Fink, Manager, Dueling Modems Computer Forum carlf@dm.net  
<http://dm.net/>

---

## ✶ The cure is only slightly worse than the disease...

"Stewart, Russell" <russtew@sandia.gov>

Wed, 21 Nov 2001 12:56:57 -0700

This story taken off of the newswire today:

[http://dailynews.yahoo.com/h/nm/20011121/od/  
tech\\_hongkong\\_champion\\_dc\\_1.html](http://dailynews.yahoo.com/h/nm/20011121/od/tech_hongkong_champion_dc_1.html)

Concerns a signal-jamming technology being developed by a Hong Kong company to block cellphone calls in areas where they are not wanted. Not a bad idea, but the following excerpt caught my attention:

"A Hong Kong company hopes to sell signal-jamming technology previously used by the military to thwart lethal missiles to block annoying cellphone calls in places such as hospitals, places of worship and restaurants."

Hospitals? Now, I admit I know very little about jamming technology, but I know that, at the very least, it requires transmitting radio energy on the same frequency as the signal you are trying to jam. Presumably, it involves transmitting at a considerably higher power than that of the target signal. Now, as I understand it, hospitals' no-cellphone policy is based on the fear that the phones' radio transmissions might interfere with hospital equipment. Are we to understand, then, that they intend to combat the problem by installing a device that, by definition, must transmit on the same frequencies at the same or considerably greater power?

I hope this was simply an error on the writer's part...

Russell Stewart, Sandia National Laboratories russtew@sandia.gov

---

## ✶ My daughter is failing high school!

"Jeremy Epstein" <jepstein@webmethods.com>

Wed, 21 Nov 2001 08:38:53 -0500

OK, you ask, what does that have to do with RISKS? Hold on a second!

Fairfax County Virginia has one school system (unlike other counties around the US where each municipality or region has their own system). My daughter goes to a magnet high school program within the county, but not the one that would ordinarily be our "home" school (i.e., the one closest to our house).

Last week she got her report card for the first quarter from the magnet school. Yesterday she got a second report card from the home school, which doesn't show any courses or grades. Luckily, it doesn't show a GPA either (I guess the programmer was smart enough not to try to average zero credit hours :-). But it does show she attended school for 40 days and was absent two days... the same number as in the magnet school.

So the county obviously has one database to record absences, but the software isn't smart enough to realize she's not taking any courses at the home school and therefore shouldn't get a report card. Or maybe that's a safeguard in case the child drops all classes without telling the parents?

I \*hope\* that when she goes to apply for college that they'll report her actual GPA, and not something silly like 0.0 since the school system obviously doesn't understand where she is! The risks of poorly designed database applications...

---

## **✶ Network Solutions ad inadvertently names my domain**

"Fredric L. Rice" <frice@skeptictank.org>

*Tue, 20 Nov 2001 14:12:52*

Back some months ago -- 11 Apr 2001, in fact -- a promotional mailer in the form of a folded post card (11 inches by 15 inches) was mailed out to who knows how many residences in Virginia (U.S.) by Network Solutions, a VeriSign Company, advertising Web site services.

Amusingly, the advertisement listed [www.squirreling.org](http://www.squirreling.org) as a sample domain name, describing a "matching e-mail address like this" with [yourname@squirreling.com](mailto:yourname@squirreling.com) as their "matching e-mail address."

Aside from the fact that Network Solutions mixed .ORG with .COM, apparently they didn't bother to check first to see whether Squirreling.ORG was an existing web site before they advertised it as an example. In fact I had registered the domain name on February 2'nd, 2000 and had acquired hosting shortly after that. The name "Squirreling" was doubtlessly picked because it sounds amusing and Network Solutions probably assumed that

nobody would  
have such a domain.

The risks? What if my web site had been something sinister?  
Network

Solutions could have suffered massive embarrassment and revenue  
losses had  
my web site contained "Bonsai Kittens" or something equally  
stupid on it.

[groups.google.com/groups?q=%22squirreling.org%  
22&hl=en&rnum=2&selm=3  
ad4add5.231072131%40news.bellatlantic.net](http://groups.google.com/groups?q=%22squirreling.org%22&hl=en&rnum=2&selm=3ad4add5.231072131%40news.bellatlantic.net)

---

## ✶ Another date risk (Re: Brown, [RISKS-21.76](#))

Leonard Erickson <shadow@krypton.rain.com>  
*Tue, 20 Nov 2001 16:49:44 PST*

Lotus and most other spreadsheets have another date risk, caused  
by trying  
to maintain compatibility with Visicalc in the original Lotus  
and carried  
over from there.

Dates are stored as the number of days since the start of 1900.  
That is Jan  
1, 1900 is stored as 1, etc. The problem is the original  
programmers thought  
that 1900 was a leap year.

Enter 60 into a date-formatted cell. Many spreadsheets will  
display it as  
Feb 29, 1900!

Microsoft Multiplan handles this by making Jan 1, 1900 store as  
2 rather  
than 1. But that means dates in it won't match dates in other

spreadsheets  
if they are before March 1, 1900.

There's no good solution anymore due to the spread of this  
"misfeature" thru  
spreadsheets across the world. All you can do is double check  
\*any\* date  
info from before 1900-03-01 that has passed thru (or may have  
passed thru) a  
spreadsheet.

Leonard Erickson (aka shadow{G}) shadow@krypton.rain.com

---

## ⚡ Re: Researchers probe Net's 'dark address space'

Arthur Smith <apsmith@aps.org>  
*Wed, 21 Nov 2001 09:49:31 -0500*

We have fallen into the accidental misconfiguration trap a few  
times for  
some of these cases -- the primary reason it happened to us is  
that routes  
advertised using "classless" IP address ranges do not get  
treated properly  
by a router that doesn't have 'ip classless' set (in Cisco-  
speak). This is  
the Classless-InterDomain Routing (CIDR) system that replaced  
the old  
Class-A, class-B, class-C hierarchy. The cable modem and  
military people  
tend to populate parts of old class-A blocks - this is any IP  
address that  
starts with a number less than 128. In our case what happened  
was we had a  
"specialty" internet provider that only provided access to  
certain networks  
which they advertised to us via the BGP protocol, and they  
filtered out any  
traffic coming from us that didn't match that list of networks.

But it turned out that some of the networks they advertised were small portions of these old class-A networks, and we naively did not have "classless" routing turned on, so our router thought the ENTIRE class-A had to be routed through them. So traffic between us and any address in that class-A block not passed through by our provider was blocked.

One reason we didn't have classless routing turned on was some previous bad experience where one of our partners' router's memory had been filled with spurious /32 routes (routes with only a single address) due to the use of classless routing, the fact that we did not have all possible routes to our own address space properly advertised to one another, and the malicious actions of some printer software that tried to scan every single address in our (class-B) address space, looking for printers.

In short, it's very easy, if you do not have much background in IP networking, to misconfigure your routers to have this sort of thing happen - and it's a little hard to spot since the network connections are generally working fine otherwise - nobody may ever complain!

---

## **✂ Glitch in iTunes Deletes Drives ([RISKS-21.74](#))**

Dave Katz <dkatz@juniper.net>

Wed, 21 Nov 2001 16:27:38 -0800 (PST)

According to a well-placed friend within Apple, the failure was a bit more complex than described. He says that the bug in the script was actually discovered prior to the software being posted, but that the corrected version somehow did not end up being posted (classic version management issue.) Furthermore, the fact that broken script had been posted was discovered in the middle of the night, but the folks responsible for the server did not pull it down until hours later, thus increasing the collateral damage (classic people management issue.)

---

## **✦ Re: FBI targets suspects' PCs with spy virus (NewsScan, [RISKS-21.77](#))**

"R.S. Heuman" <rsh@idirect.com>  
*Wed, 21 Nov 2001 18:32:27 -0500*

And of course no self-respecting non-US anti-virus firm is going to put a signature into their product that will detect and report on this trojan? Somehow the first time it is detected by anyone it will get into F-Prot, F-Secure, AVP and a number of other non-US products that are widely used even in the US, and then what? If the AV product vendors ignore this software, they are in for attack from their customers, and if they detect it they are in for attack from the FBI?

Which would you choose were it your corporation? This type of program and

its detection is too much of a risk for the FBI for them to widely disseminate it, and ignoring such a program is too much of a risk for the AV product vendors to accept, since alienating their clients will unfortunately result in a major downturn in their corporate viability, once it becomes known, which will be almost immediately.

---

**Re: FBI targets suspects' PCs with spy virus (NewsScan, RISKS-21.77)**

Rob Slade <rslade@sprint.ca>

Wed, 21 Nov 2001 15:41:40 -0800

> The FBI is working on software that could insert a computer virus ...

First off, nothing about this program indicates that it is a virus. There is nothing about reproduction in the description. In any case, a virus would be a fairly imprecise way of delivering a security breaking package (although steps could be taken in that regard).

> suspect's computer capable of reading encrypted data.

As the later material shows, the program is not capable of reading encrypted data, it simply steals passwords. Fairly common activity for trojans in past years.

> The software, known as "Magic Lantern," installs "keylogging" software

> that can capture keystrokes typed on a computer. The virus

can be sent  
> via e-mail.

As Peter notes, Microsoft Outlook is somewhat susceptible to this type of thing, but in pretty much every other case you'd have to convince the target to run an attachment. That might be a little trickier. "The attached Microsoft Word document contains an application form for our special Kali cartel `frequent pusher' discount, good for an extra 10% off on shipments of 100 kilos or more." "Run this hilarious screensaver with inspirational (secret) messages from our beloved leader Osama, along with detailed instructions on the construction of truck bombs."

[But this seemed to happen all the time with IL\*V\*Y\*\*, etc. PGN]

The targeting of PGP is interesting. Does this mean that the US government is still ticked over its creation, or that they are finally (tacitly) admitting that open-source software really *is* more secure?

> ... possible to observe every keystroke typed by the suspect, even if a  
> court order specified only encryption keys.

It would certainly be easier to collect information, particularly for ephemeral data, such as e-mail. On the other hand, how are the authorities supposed to get at the data? I suppose sending out only the passphrase would be less suspicious if someone was keeping track of traffic. (On the other hand, if anyone was logging port activity it would be fairly easy to scan for Magic Lantern in the same way that people scan for Back Orifice,

SubSeven, Bionet, and other RATs.)

> [Insertion by e-mail probably works well for Microsoft  
software, which is  
> prone to that kind of attack. Various reports suggest that  
Magic Lantern  
> can also plant itself by penetrating systems.

Penetrating how? I would hope that the RISKS audience is  
somewhat less  
suggestible, along these lines, than the general public. [You  
must be  
kidding! PGN]

> Penetrability of supposedly secure systems has long been  
noted here ...

True, but the penetration is still probably going to happen on a  
case by  
case basis. Viruses would be a good way to break  
confidentiality (just look  
at Sircam), but are rather a blunt instrument, tending to drown  
signal with  
noise (look at Noped).

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)

---

## **RISKS-21.77 was rejected by some filters**

<PGN>

*Wed, 21 Nov 2001 19:07:42 PST*

[RISKS-21.77](#) contained a string naming a recent virus "IL\*V\*Y\*\*".  
Some of you apparently have filters that are so lame they cannot  
tell

the difference between that spelled out in text and the actual virus.

Overzealous filtering is rapidly becoming a bad joke.

---

## **✉ Re: Porn spam being sent in my name (Sanders, [RISKS-21.76](#))**

Andrew Klossner <andrew@cesa.opbu.xerox.com>

*Wed, 21 Nov 2001 07:17:02 -0800*

> Imagine my surprise to find that the original (bounced) message had

> been spam, apparently sent from me!

That "original message" was never sent. The "bounce notification message" was forged by the spammer. And it worked -- you paid close

attention to it.

---

## **✉ Re: Programming error ... (Stein, [RISKS-21.77](#))**

<dgillett@deepforest.org>

*Wed, 21 Nov 2001 15:08:06 -0800*

> The best folks prefer product engineering (aka 'development').

I don't believe this is true at all.

I believe that the vast majority of employees, and many managers, in the computer field regard product engineering as the "senior" department, the superior order amongst technical professionals. [That upper management often considers sales to outrank all technical groups takes a

while to  
discover....] The result is that other technical departments,  
such as QA  
and IT, are often staffed largely with junior engineers bidding  
their time  
and acquiring years of experience to try to get into product  
engineering.  
Naturally, they're not very good at what they're currently being  
paid to do  
-- they'd much prefer to be in product engineering -- but  
they're not  
necessarily any better at *\*it\**. On the counter side, there  
*\*are\** a few  
excellent, committed QA and IT and Tech Support folks around --  
"the best"  
in these realms -- and often that is intimately tied to their  
discovery of a  
personal preference for one of these "ancillary" roles.

I would say that the *\*majority\** prefer product engineering --  
and that this  
is linked, chicken-and-egg fashion, to other branches being  
under-appreciated and staffed largely by inexperienced,  
uninterested, and  
(as a consequence) ineffective personnel. The consequences? We  
read about  
them on the RISKS Digest every week.

David Gillett

---

## **✉ Re: Toaster failures (Re: Hackett, [RISKS-21.76](#))**

Marcus Didius Falco <marcus\_d\_falco@yahoo.com>

*Tue, 20 Nov 2001 14:20:15 -0500*

According to the Dec 2001 issue of *\*Consumer Reports\**, your  
problems with  
toasters are not unique, and they were able to get better toast

from some  
simpler toasters (that is, without all the sensors).

However, the risk of toasters not turning off until they have  
popped has  
been addressed in the US. There is now a Consumer Product Safety  
Commission  
standard requiring toasters to turn off when the cycle is over,  
whether or  
not the "pop" has occurred. It takes effect for toasters  
manufactured after  
November 2001, but many toasters are now compliant (and some  
actually give  
some indication of this compliance on the box).

---

## ⚡ The more things change

<albaugh@spies.com>

*Tue, 20 Nov 2001 14:49:17 -0800 (PST)*

In [RISKS-21.76](#), we read about (800)555-1212 re-directing  
information  
calls. Those familiar with the history of the telephone system  
may recall  
that Almon P. Strowger, generally regarded as the inventor of  
automatic  
telephone switching apparatus (at least in the U.S.A. :-)) was an  
undertaker,  
who produced his invention because he was tired of the telephone  
operator in  
his town "accidentally connecting" his calls to his competitor,  
said  
operator's husband. Of course, all those helpful Web "directory"  
sites have  
been doing this for years, and "Smart-Links" threatens to move  
the betrayal  
right to your PC. (Yes, I know, not right now, yet...)

We also read about:

> Subject: Re: Another SRI-wide power outage (Rowland, [RISKS-21.74](#))

>

> [...] The Xerox tech would decide that the the pair of side by side tops of

> the controllers made an excellent surface for him to flop his huge folder of

> tech charts onto, toggling the power switches on both modems off.

Which reminded me of the result of using the oh-so-convenient top of the IBM

1401's Core-memory extension to set down 7-track mag-tapes temporarily,

until we figured out why we where getting so many errors... (We put a

two-drawer steel card-file on top, and added a notice under that file

explaining the issue and saying "Put it back")

---

## **★ Re: IP: 800 directory "assistance" redirecting calls (Glass, [R 21 77](#))**

Rob Bailey <wl2000@newsguy.com>

*Tue, 20 Nov 2001 11:30:29 -0800 (PST)*

Brett Glass's story on operator-assisted dialing that resulted in customer

hijacking would probably have shocked Almon Strowger, the funeral parlor

manager who, as the story is told, invented the Strowger switch, which as we

all know would become the backbone for the electromechanical direct-dial

apparatus in place for many decades. (As the story is told, Strowger

[STRO-jer] suspected the local telephone exchanges of routing potential customers [well, I suspose the families of potential customers!] for his funeral parlor to his competitors' parlors. Paranoia was the mother of Strowger's invention.)

As long as callers leave the recipient-to-number translation in the hands of others, for convenience of any other reason, this problem will likely persist.

Rob Bailey, wm8s@pobox.com

---

**[Re: 800 directory "assistance" redirecting calls \(Glass, RISKS-21.76\)](#)**

Clay Jackson <clayj@nwlinc.com>  
*Wed, 21 Nov 2001 09:12:43 -0800*

The risk was not properly identified.

While this is certainly an issue; IMHO Bret has the risk all wrong. This is a classic case of 'Never attribute to malice what can be explained by stupidity'. I'm sure AT&T (I'm assuming here, since they're the biggest user of TellMe) made NO deliberate attempt to 'hijack' the hotel's number (what possible benefit would ANYONE receive from rerouting a caller looking for a hotel to a furniture store). What's much more likely is that the TellMe VR software made a mistake; or, that it doesn't handle duplicate names very well.

## ✉ Re: National ID cards (Shostack, [RISKS-21.75](#))

Henry Baker <hbaker1@pipeline.com>

*Tue, 20 Nov 2001 19:47:17 -0800*

I'm not going to comment on national ID cards directly, but only upon Adam Shostack's reasoning. Every web page (instruction, datum, etc.) is accessed a first time, as well, but caches still work pretty darn well on a statistical basis.

Screening will always be a statistics game, but we need to attach wildly different costs to various kinds of screening misses. Clearly, 20 box cutters can ruin a lot of days. The IBM 360/30 didn't execute a "divide" instruction or a "convert to decimal" instruction very often, but when it did, they was so slow that they often dominated instruction trace timings. So the next generation of 360's improved the execution speed of those particular instructions.

However, much of the improvement in computer execution speeds over the past twenty years is the result of tuning to more broadly valid statistical data, rather than focusing only on rare but costly instructions. Similarly, we need to continue to make flying as a whole safer, rather than focus only on the threat of terrorism, as the recent NYC crash sadly proves.

## **⚡ Re: Windows XP accounts by default are administrator with no password**

Mark Wilkins <mwilkins@pdi.com>

*Tue, 20 Nov 2001 10:54:48 -0800*

> If you create user accounts, by default, they will have an  
account type of  
> Administrator with no password."

This is probably a result of aggressive product management.

Some years ago I worked for Mitsubishi Consumer Electronics in  
their  
software department, and was tasked to write the code to  
implement  
parental lock on a (now long defunct) chassis of TV set.

I'd implemented it so that all the settings would remain as  
parents locked  
and unlocked the TV, so that parents could set all their  
settings for each  
channel once and allow or deny TV viewing according to those  
settings as  
they liked.

Much of that logic had to be re-implemented for a different  
behavior:  
unlocking the TV caused ALL of the information about which  
channels or times  
were or were not permissible to be erased, requiring that they  
be re-entered  
next time.

The reason for this was that apparently support telephone calls  
on the issue  
of parental lock nearly never asked the question "Why can't I  
lock my kids  
out of the television?" and instead nearly always asked "My kids  
have locked

me out of the television. What do I do?" Since those calls cost money to support a product for which the company had already been paid, they were to be minimized. The product had to be easy to unlock and hard to lock.

I suspect this behavior in Windows XP is a similar matter.

---

## ✶ Let's get really paranoid about e-mail and spam...

"Allan Hurst" <allanh@supportnet.com>

*Tue, 20 Nov 2001 11:54:57 -0800*

Re: Porn spam being sent in my name (Sanders, [RISKS-21.76](#))

Here's how much worse it can get: In the past couple of years, I've opened up e-mail accounts on three different systems: Yahoo Mail, HotMail, and MyRealBox.com.

These accounts were used ONLY for testing internet e-mail gateways on new e-mail systems that we set up for clients They have never been used for posting to a list, responding to an ad, and/or have never been entered into any Web site.

- Within two months of opening the Yahoo! Mail account, it started receiving spam, none of it from Yahoo.

- Within three days of opening the HotMail account, it started receiving spam, in amounts far larger than the Yahoo account.

In both of the above cases, I had specifically selected to NOT be listed in either of the systems' directories, and to NOT receive e-mail offers from any of their "marketing partners". Neither of these accounts were ever used to respond to offers, entered into Web sites, or published anywhere. They were only used to send and receive test e-mail messages to and from new e-mail servers.

Either Yahoo Mail and HotMail are lying about not publishing or selling addresses, or someone's harvesting e-mail addresses by sniffing packets.

(Hence the subject of this message.) As much as I'd like to bash the vendors ... I strongly suspect the answer is that someone's found a way to harvest e-mail addresses. (Keep reading.)

I next opened up a third test account, on MyRealBox.com. This is a demonstration mail service operated by Novell, Inc., to show off its NIMS product, and having met people from the NIMS team at various Novell functions, I had been informed that they specifically do NOT sell the MyRealBox accounts, nor use them for marketing purposes of any kind.

For about six months, I received no spam of any kind on the MyRealBox account. Suddenly, I was flooded with everything from "failed delivery" messages to angry missives threatening me with bodily harm for spamming them.

Some of the missives included the complete message, which was a piece of

spam generated with my MyRealBox account name in the "From" and "Reply-To" fields! The messages did NOT originate from MyRealBox, however, nor did they pass through any "traceable" intermediate mail servers (only IP addresses were shown in the headers).

This raises the question: if the MyRealBox account name wasn't sold (and I believe it wasn't), then how on earth did the spammers "harvest" my specific MyRealBox account name to use to send spam with? (And are there any steps one can take to prevent it from happening again?)

This also brings to mind the risk of using a "free" internet e-mail account, or any type of outsourced e-mail server over which one has no legal or authoritative control.



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 21: Issue 79**

**Tuesday 27 November 2001**

## Contents

- [Harry Potter related risks](#)  
[Richard Akerman](#)
- [Phone banking hiccups](#)  
[Geoffrey Brent](#)
- [Risks of the space character in Unix filenames](#)  
[Diomidis Spinellis](#)
- [FBI: home-grown terrorists](#)  
[Scrounger](#)
- [Misdirected criticism of Google](#)  
[Chris Adams](#)  
[Gary McGraw](#)
- [Re: Mobile phone jamming](#)  
[Markus Kuhn](#)
- [Re: Stupid virus filters](#)  
[Leonard Erickson](#)
- [Re: Let's get really paranoid about e-mail and spam](#)  
[Skip La Fetra](#)
- [REVIEW: "The CISSP Study Guide", Ronald L. Krutz/Russell Dean Vines](#)  
[Rob Slade](#)
- [Info on RISKS \(comp.risks\)](#)

## ✶ Harry Potter related risks

Richard Akerman <rakerman@bigfoot.com>

*Fri, 23 Nov 2001 19:51:14 -0400*

I went to see the Harry Potter movie. There was a long line at the box office, but none for the self-serve machines, so I went ahead and used the self-service (which I prefer anyway). No problem, I got to the final screen showing the price, it asked me to swipe my credit card and I did. Then I waited... and waited. The screen stayed up and the card reading device just kept saying "WELCOME / BONJOUR" over and over again. Eventually an employee came up and told me that the machines weren't working - in fact their entire computer system was down - the long line at the box office was because no one could purchase tickets.

\* Risk 1: Kiosks that let you get to final purchase stage even though

purchasing is not possible.

\* Risk 2: Employees who don't move to prevent access to such kiosks quickly enough.

\* Risk 3: A ticket office that shuts down completely when the computers are down

However, the end result, while risk-full, was actually handled quite gracefully. After waiting in line for a while, I went back to check on the kiosk, and a different employee said a ticket had printed out when the

computers came back up, and he had given it to the manager. I showed my credit card to the manager and he gave me my ticket.

Risk 4: A kiosk that stores a transaction and then completes it many minutes later when the main computer system/network comes back up!

However, kudos to the quick-thinking second employee, who handled the situation of an unexpected ticket coming out of the kiosk fairly well.

[Sort of a rushin' roulette-like situation? Perhaps a Pottery-wheel? PGN]

---

## **⚡ Phone banking hiccups**

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

*Tue, 27 Nov 2001 14:22:36 +1100*

On 5 Nov 2001, I tried to use the National Australia Bank's phone banking system to transfer money from my cheque account to pay off my credit card.

As prompted by the automated menu system, I entered my user number and PIN, and requested this transfer. Only after I'd confirmed the transfer was I told "phone banking is unavailable at this time, your transaction could not be processed." I called back later in the day, this time successfully completing the desired transfer.

Some weeks later I received my latest credit-card statement... and discovered that *\*both\** transactions had in fact been processed,

despite the  
message I received first time around.

Besides the obvious annoyance value and possible inconvenience of transferring more money than I'd intended, this behaviour strikes me as a security weakness. From the user end, a system that requests password data but is unable to provide the services that password should access looks suspiciously like a password-grabber. A system that accepts a password and tells the user that no transaction has been made, while debiting their account, looks even more suspicious.

Legitimate software should, wherever possible, avoid resembling malware -- even in its failure modes. Training users to accept suspicious behaviour as the norm makes the system much more vulnerable to deliberate abuse.

Geoffrey Brent

---

## ✶ Risks of the space character in Unix filenames

Diomidis Spinellis <dds@aueb.gr>

*Thu, 22 Nov 2001 23:50:39 +0300*

The root of the problem reported in the "Glitch in iTunes Deletes Drives (Solomon, [RISKS-21.74](#))" article is the default way the Unix shell handles filenames with embedded spaces. Although a space can legally appear in a Unix filename, such an occurrence is not usual; Unix filenames tend to be

terse, often even shorter than a single word, (e.g. "src", "doc", "etc", "bin") so they can be swiftly typed. A number of more recent and supposedly user-friendly operating systems like the Microsoft Windows family, and, I understand, the MacOS, use longer and more descriptive file names ("Documents and Settings", "Program Files"). Many of these filenames contain spaces; the ones I listed are by default used by Windows 2000 as the location to store user data and application files (the equivalent of /home/username and /bin under Unix).

As Unix-style tools and relevant applications are increasingly ported to run under Windows (see for example [1, 2, 3] and my Windows outfit tool suite described in [4]) or natively run under Mac OS X, problems and associated Risks arise. The main reason is that some often-used Unix shell constructs fail when applied to filenames containing a space character. Unfortunately, these constructs appear in many existing programs, and even in the writings of the original system developers, who, in all fairness, could not have foreseen how their tools would have been used 25 years after their conception.

Technically, the problem manifests itself when field splitting (the process by which the shell splits input into words) is naively applied on the output of an expansion that generates filenames with embedded spaces. Consider the following example, appearing on page 95 of one of the classic texts on Unix programming [5]:

```
for i in ch2.*
```

```

echo $i:
diff -b old/$i $i
echo
done

```

The above code will compare all files matching the `ch2.*` pattern in the current directory with copies presumably stored in the directory called

"old". Consider what will happen when the code is applied to a file called "ch2.figure 3.dot" (notice the space between the word figure and the "3").

The shell variable `i` will be set to the correct filename, but then the shell will execute the "diff" command with the following argument list (customarily passed to C programs in the `argv` array):

```

argv[0] = "diff"
argv[1] = "-b"
argv[2] = "old/ch2.figure"
argv[3] = "3.dot"
argv[4] = "ch2.figure"
argv[5] = "3.dot"

```

and `diff` will complain

```
diff: extra operand
```

as more than two filenames were passed as arguments. This happens,

because words are expanded by most Unix shells in the following order:

1. Parameter (including variable) expansion, command substitution.

2. Field splitting.

As a result, the variable `$i` is first expanded into "ch2.figure 3" and

then the result is split into fields for further processing or for

passing them as arguments to a command.

The most common dangerous constructs that can appear in step 1 are variable references (e.g. `$PATH`, `$word`) and commands inside backquotes (e.g. ``find`

. -type f -name 'ch2.\*'`). These dangerous constructs are quite common, appearing among other places in the original article describing the Bourne shell [6] (for i in \* do if test -d \$d/\$i [...]), in other scripts in the reference of the original example [5 p. 141, 143], and even in quite recent work by the same authors [7, p. 149]. It is also prevalent in existing operating system tools; I counted 43 occurrences of one suspicious pattern ("\$\*") in a NetBSD source tree, 8 in a FreeBSD command path, and 49 in the shell scripts of a Mandrake Linux distribution. The Unix world is definitely not ready to deal with filenames containing the space character.

Avoiding this problem is not trivial. A radical solution would be to change the value of the shell's "internal field separator" (IFS) variable. This variable contains the characters that shell uses to split words. Its default value is "<space><tab><newline>". This solution however would break more things than it would fix, since most scripts expect words to be separated by spaces. As an example the construct "A='ls -l';\$A" would not work. The most practical solution is to manually enclose variables inside double quotes when using them in contexts where only a single word is normally expected. The shell will still expand the variable inside the quotes, but will treat the result as a single word. Thus the offending part in the original example should have been written as:

```
diff -b "old/$i" "$i"
```

In addition, whenever a shell script uses the variable \$\* to obtain the

values of all parameters passed to a script, the `$*` variable should be replaced by the variable `$@`, again inside double quotes. Thus the

common code pattern

```
for arg in $*
should be written as
```

```
for arg in "$@"
```

Interestingly, Kernighan and Pike were aware of the `$*` problem and the above

solution since 1984; they aptly characterize the `"$@"` solution as "almost

black magic" [5 p. 161].

Still, these changes will not correctly handle filenames with embedded

whitespace returned from a command substitution. In this case, temporarily

changing the IFS variable before executing a command may be the only

feasible solution. The following example illustrates this approach:

```
# Save original IFS
```

```
OFS="$IFS"
```

```
# Set IFS to newline
```

```
IFS='
```

```
'
```

```
# The find command might output filenames with spaces
```

```
wc -l `find . -type f`
```

```
# Restore original IFS
```

```
IFS="$OFS"
```

By searching existing shell scripts for the patterns I described and

applying the suggested changes most problems can be solved.

Other scripting

languages like Tcl and, to a lesser extent, Perl may also have problems

dealing with filenames with spaces. Similar approaches

(appropriate quoting

in Perl "eval" blocks and use of the "list" command in Tcl) can be used to

avoid these problems.

## References

- [1] David G. Korn. Porting Unix to Windows NT. In Proceedings of the USENIX 1997 Annual Technical Conference, Anaheim, CA, USA, January 1997. Usenix Association.
- [2] Geoffrey J. Noer. Cygwin32: A free Win32 porting layer for UNIX applications. In Proceedings of the 2nd USENIX Windows NT Symposium, Seattle, WA, USA, August 1998. Usenix Association.
- [3] Stephen R. Walli. OPENNT: UNIX application portability to Windows NT via an alternative environment subsystem. In Proceedings of the USENIX Windows NT Symposium, Seattle, WA, USA, August 1997. Usenix Association.
- [4] Diomidis Spinellis. Outwit: Unix tool-based programming meets the Windows world. In USENIX 2000 Technical Conference Proceedings, pages 149-158, San Diego, CA, USA, June 2000. Usenix Association. <<http://www.dmst.aueb.gr/dds/pubs/conf/2000-Usenix-outwit/html/utool.html>>
- [5] Brian W. Kernighan and Rob Pike. The UNIX Programming Environment. Prentice-Hall, 1984.
- [6] S. R. Bourne. The UNIX shell. Bell System Technical Journal, 57(6):65-84 July/August 1978. (Also appears in volume 2 of the Unix Programmer's Manual and in AT & T, UNIX System Readings and Applications, volume I. Prentice-Hall, 1987.)
- [7] Brian W. Kernighan and Rob Pike. The Practice of Programming. Addison-Wesley, 1999.

Diomidis Spinellis - <http://www.dmst.aueb.gr/dds/>  
Athens University of Economics and Business (AUEB)

---

## **✶ FBI: Home-grown terrorists**

Scrounger <scroungr@nightfall.forlorn.net>

Wed, 21 Nov 2001 22:14:30 -0800

[RISKS-21.77](#) remarks on the FBI installing a program that logs keystrokes on a suspect's computer "FBI targets suspects' PCs with spy virus", which I'm sure most would agree damages it. Of course, [RISKS-21.76](#), in "Re: Kids' learning game site becomes porn site (Smith, [RISKS-21.74](#))" includes a link to the US PATRIOT Act <<http://www.zdnet.co.uk/itweek/columns/2001/42/bingley.html>>, which defines such damage as terrorism. So the FBI is a terrorist organization... Who knew?

---

## **✶ Misdirected criticism of Google (Re: [RISKS-21.75](#))**

Chris Adams <chris@improbable.org>

Tue, 27 Nov 2001 01:20:36 -0800

<http://news.cnet.com/news/0-1005-202-7946411.html>

Google keeps improving and people are starting to find sensitive information they put online isn't as private as they thought - they had relied on the traditional opacity of proprietary formats to keep it out of search engines, if they thought of it at all. The solution? Blame Google.

As if it wasn't bad enough that many normal users don't understand that

putting information online makes it available to the public,  
consider the  
expert authority CNET quoted:

> "We have a problem, and that is that people don't design  
software to  
> behave itself," said Gary McGraw, chief technology officer of  
software  
> risk-management company Cigital, and author of a new book on  
writing  
> secure software.  
>  
> "The guys at Google thought, 'How cool that we can offer this  
to our  
> users,' without thinking about security. If you want to do  
this right,  
> you have to think about security from the beginning and have a  
very  
> solid approach to software design and software development  
that is  
> based on what bad guys might possibly do to cause your program  
grief."

McGraw doesn't seem to understand the rule he's parroting. That  
maxim is  
correct - people don't spend enough time considering unusual or  
hostile  
behaviour when designing software - but he's completely wrong  
about the  
guilty party: access control is the responsibility of the  
publisher, not the  
indexer. Basic information theory teaches that someone can use  
data in any  
way they choose if they can get it in any usable form - the only  
way to  
prevent this is to keep them from getting it in the first  
place. (I'm  
reminded of Bruce Schneier's observation that trying to prevent  
this is like  
trying to prevent water from being wet.)

The risks?

- Attacking companies like Google will hinder innovation while

doing nothing to improve actual security.

- Misdirected blame may lead to misguided legislation like the proposed SSSCA, mistakes which will be enormously expensive to correct.
- Companies will continue to rely on security experts who don't understand the theories behind the guidelines they repeat. Watching the server logs while clients were being audited by certain large firms has convinced me that there's almost no value in such certifications.

---

## ✶ **Misdirected criticism of Google (Adams, [RISKS-21.79](#))**

Gary McGraw <gem@cigital.com>

*Tue, 27 Nov 2001 17:48:29 -0500*

I completely agree with Chris. In fact, I have long been a proponent of the rule that I have been accused of "parroting" (as many of you guys know).

And I certainly hope I understand at least some of the theories behind the guidelines. I invite Chris to see for himself by reading "Building Secure Software" (Addison-Wesley 2001).

I actually made a number of similar points during the long interview, but

the reporter seems to have latched on to a twisted version of what I meant.

Alas, this happens all the time. It's one of the classic RISKS of talking to the press!

Nevertheless, the RISK that Chris pointed out (misdirecting

blame) is a valid one and deserves some airplay here on RISKS. I rest my case.

---

## ✉ **Re: Mobile phone jamming (Stewart, [RISKS-21.78](#))**

Markus Kuhn <mgk25@cl.cam.ac.uk>

*24 Nov 2001 21:42:34 GMT*

>... Now, as I understand it, hospitals' no-cellphone policy is based on  
>the fear that the phones' radio transmissions might interfere with hospital  
>equipment.

The above is a common misconception about how mobile phone jammers work.

They attempt to suppress reception of the base station transmitter signal by the mobile unit receiver, as this requires orders of magnitude less energy than jamming the other way round. The jammer only has to be slightly stronger than the nearest base station (which is usually hundreds of meters away and outdoors) and if properly designed and installed will not increase ambient field levels significantly. In particular, a jammer does not have to be anywhere near as strong as a nearby handset!

Mobile phone jammers for GSM and other standards have been on the market for many years and the users of the handheld variants enjoy a much longer battery lifetime than their nearby victims. The simplest GSM jammers just wobble a carrier across the 935-960 MHz band to

disrupt

the base station signal, whereas the mobile phones transmit much stronger in the 890-915 MHz range.

The no-cellphone policies in hospitals are today mostly based on the fear

that clueless phone users might operate phones in the immediate vicinity

(with a couple of centimeters) of critical equipment. As soon as the mobile

phone is a few meters away, field strength will drop well beyond the 3 V/m

levels against which medical equipment has to be EMC immunity tested by the

manufacturers (EN 50082, IEC 601-1-2).

Markus G. Kuhn, Computer Laboratory, University of Cambridge, UK  
mkuhn at acm.org, WWW: <<http://www.cl.cam.ac.uk/~mgk25/>>

---

## ✶ Re: Stupid virus filters (Re: [RISKS-21.77](#))

Leonard Erickson <shadow@krypton.rain.com>

*Fri, 23 Nov 2001 16:02:27 PST*

> ... Overzealous filtering is rapidly becoming a bad joke.

I had a message to some friends bouncing as containing "bad data" in the message body or some such uninformative diagnostic. I finally contacted my uucp feed about it, and found that the problem was just such a filter. But rather than being in the \*body\*, the problem was in the \*header\*.

He was filtering for a subject of "Gunny" or "Funny joke" (I forget which) because "too many viruses/trojans are using that subject".

Argh!

Leonard Erickson (aka shadow{G}) shadow@krypton.rain.com

---

## **⚡ Re: Let's get really paranoid about e-mail and spam (Hurst, [R 21.78](#))**

"LAFETRA,SKIP (HP-SantaClara,ex3)" <skip\_lafetra@hp.com>

*Sun, 25 Nov 2001 12:13:01 -0500*

In [RISKS-21.78](#), Allan Hurst relates how he opened e-mail accounts used only for testing, and within a month started to receive SPAM.

I can confirm his story. A few months ago I opened a HOTMAIL account which was NEVER used for ANY purpose, and whose existence was not told to ANYBODY. (For the curious, I intended to do some Passport testing which I never got around to performing).

Within two weeks, this HOTMAIL account (with an unusual name -- 5 characters with an embedded numeral [the really curious can look up my "ham" radio callsign and send me mail] was receiving pornographic SPAM.

In all of history, I have sent ONE message from this account -- to abuse@hotmail.com -- after the SPAM started. At the present time, this account receives roughly a half-dozen SPAM (about 90% sexual) per day. This account has also receive three (3) messages from HOTMAIL administration advertising extended features (which I class as legitimate mail).

I have had friends speculate that spammers "accidentally" found this account through a random search. Frankly, I don't believe them, and think that it is more likely that an "information leak" within the hosting organization has provided this address to spammers, or that some form of packet sniffing has found my (occasional -- about every-other-week) logins to see what has arrived at the account. Like Mr. Hurst, I took great pains to exclude this account from any directories or "send me mail from affiliate" selections. Unlike Mr. Hurst, my account has NEVER been used or communicated for any purpose.

Skip La Fetra (Skip@LaFetra.com)

---

## **⚡REVIEW: "The CISSP Study Guide", Ronald L. Krutz/Russell Dean Vines**

Rob Slade <rslade@sprint.ca>  
*Thu, 22 Nov 2001 08:00:13 -0800*

BKCISPPG.RVW 20010924

"The CISSP Study Guide", Ronald L. Krutz/Russell Dean Vines, 2001,  
0-471-41356-9, U\$69.99  
%A Ronald L. Krutz  
%A Russell Dean Vines  
%C 5353 Dundas Street West, 4th Floor, Etobicoke, ON M9B 6H8  
%D 2001  
%G 0-471-41356-9  
%I John Wiley & Sons, Inc.  
%O U\$69.99 416-236-4433 fax: 416-236-4448

%P 556 p.

%T "The CISSP Study Guide: Mastering the Ten Domains of Computer Security"

Of late there has been a significant increase in interest in the CISSP (Certified Information Systems Security Professional) exam and designation produced by the (ISC)<sup>2</sup> (International Information Systems Security Certification Consortium). The CISSP exam is based on the Common Body of Knowledge (CBK) which, as the name implies, is that information assumed to be customarily known by those qualified or experienced in the field of computer security. Since the (ISC)<sup>2</sup> also runs courses based on the CBK, many people seem to feel that there is some trick or secret to passing the exam.

Krutz and Vines appear to want to foster this myth, since the first sentence of the introduction states that this book holds the "key to unlocking the secrets of the world of information systems security." If true, this assertion would make a mockery of the (ISC)<sup>2</sup> requirement for three years' work experience, and the insistence that no one book holds the entire CBK.

The introduction also states that this work is intended as a preparatory guide for CISSP students, a reference for students of other information security courses, and a manual in security basics and emerging technologies for security professionals. That's a rather tall order.

For those who have seen the (ISC)<sup>2</sup> CBK course materials, it is immediately

obvious where the structure of the book, and most of the content, originates. Much of the text is in point form, following the slides used in the CBK, with only minor expansion to explain the elements. Discussion of concepts is limited, and some of the detail provided is of questionable value. In addition, while the CBK is a substantial and useful work, the (ISC)<sup>2</sup> course structure does suffer, over time, as areas are added or amended, and the strict adherence to that order, which can be smoothed over in a seminar, makes the book very jumpy in places. Security management practices, in chapter one, is rather choppy, and access control, in chapter two, is even worse in this regard.

Each chapter covers one of the ten domains of the CBK. These topics tend to overlap in places, but there is little attempt to explain, reconcile, or reference duplicated material. Both chapter two and telecommunications and network security, in chapter three, address intrusion detection systems, but neither section refers to the other. (Telecom and networks is a large topic, and would have benefitted from some attempt at reorganization.)

Chapter four describes many details of cryptography. While the particulars provided are correct, the lack of background reduces the value of the text. Security architecture and models, in chapter five, defines most of the terms, but does not give a complete picture of the topic. Operations security generally involves the coordination of a number of individually simple aspects, so chapter six deals with the topic adequately.

The same minimalist denotation of points does not work as well for applications and systems development, in chapter seven. (In addition, it is disturbing to see that discussion of viruses has been completely excluded, particularly in view of the fact that the subject has greater representation in the CISSP exam than in the CBK course itself.) Again, business continuity and disaster recovery planning involve a number of basic operations, so chapter eight provides reasonable coverage. Chapter nine's review of law, investigation, and ethics is terse, but not out of line with the requirements of the exam. Physical security, in chapter ten, is covered better than most other areas.

There are a number of appendices. A glossary is taken from the old (1985) US government glossary, with a few additions. There is an overview of the old "Rainbow" series of security manuals. An essay on using the Capability Maturity Model (CMM) with the Health Information Portability and Accountability Act (HIPAA) will possibly be of interest to a very select group. There is an overview of the National Security Agency (NSA) Infosec Assessment Methodology, a simplistic look at penetration testing, and a ludicrously brief list of the contents of British Standard 7799. The examination of the Common Criteria is slightly better, but not sufficient to address the needs of the CISSP exam. A list of references for further study is basically taken from the (ISC)<sup>2</sup> resource list with some added URLs, and is not annotated.

Oddly, the illustrations are not copied from the CBK course, and table and section headings relate very poorly to the surrounding text.

Practice with sample questions can be important in preparing for the CISSP exam. Those provided by the CBK course, and even the independent [www.cccure.org](http://www.cccure.org) site, are very similar in tone, style, and difficulty, to those on the exam. The specimen questions in this book, however, are not.

The quizzes are simplistic reading checks and definition queries, with none of the complexity of the exam, and requiring little in the way of judgment.

The full list of questions is given again in appendix C, with answers: the solutions are sometimes explained, but often are not.

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.

copyright Robert M. Slade, 2001    BKCISPPG.RVW    20010924  
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 21: Issue 80**

**Saturday 1 December 2001**

## Contents

- [Badtrans "worm" can capture keystrokes](#)  
[NewsScan](#)
- [Records stolen in Auckland](#)  
[Richard A. O'Keefe](#)
- [Calif info: Ask and you shall be removed ... but you've got to ask](#)  
[NewsScan](#)
- ["Light turnout" for election](#)  
[G R Rhodes](#)
- [The destruction of 7 WTC](#)  
[Jacob Harris](#)
- [Connecticut Attorney General website wants Microsoft browsers?](#)  
[Ed Ravin](#)
- [How to crash a phone by SMS](#)  
[Monty Solomon](#)
- [The Web Never Forgets](#)  
[Monty Solomon](#)
- [Risks of computer security education](#)  
[David Friedman](#)
- [Re: Let's get really paranoid about e-mail and spam](#)  
[Walter Dnes](#)

[Jason Bennett](#)

● [Re: Risks of the space in Unix filenames](#)

[David A. Moon](#)

[Richard A. O'Keefe](#)

● [REVIEW: "Hackers Beware", Eric Cole](#)

[Rob Slade](#)

● [Info on RISKS \(comp.risks\)](#)

---

## ⚡ **Badtrans "worm" can capture keystrokes**

"NewsScan" <[newsscan@newsscan.com](mailto:newsscan@newsscan.com)>

*Tue, 27 Nov 2001 08:28:53 -0700*

A malicious program called Badtrans is moving around the Internet and worming itself into vulnerable computers and using a keystroke logger to surreptitiously record passwords, credit data, and other information. A virus manager at the security firm McAfee says that the worm "does no damage to files but does drop a backdoor trojan on the machine which would allow a hacker to come back and access personal information." Badtrans spreads through Microsoft's Outlook or Outlook Express e-mail programs and arrives with an attachment that can be executed simply by reading or previewing it and doesn't need to be double-clicked or opened separately.

[Reuters/\*San

Jose Mercury News\*, 27 Nov 2001; NewsScan Daily, 27 Nov 2001]

<http://www.siliconvalley.com/docs/news/svfront/034639.htm>

[Incidentally, we received a lot of e-mail on Magic Lantern. Let me

summarize a little. Rob Slade questioned whether it was a virus in

[RISKS-21.78](#). This is an old battle, because "virus" has become overloaded. Peter da Silva and PGN both insist it is a Trojan Horse.

Let's get on with it, and use the terminology correctly. There was some

discussion on whether or not McAfee et al. will suppress detection of an

FBI-planted virus, vague denials. There were some comments about ML being

used only against bad guys, so what's the problem (slippery slope there).

Tony Harminc remarked that collection need not be real-time if a Trojan

horse is collecting the info for later dissemination. Dave Farber

wondered about the possibility of disguising a really nasty virus so that

it would slip through the mechanism that intentionally failed to detect

ML. Several folks resurrected the old argument that the ability to insert

malware actually weakens security. PGN]

---

## ✶ Records stolen in Auckland

"Dr Richard A. O'Keefe" <ok@cs.otago.ac.nz>

Thu, 29 Nov 2001 14:24:35 +1300

Thousands of people's financial details have been stolen in a myster

burglary in Auckland. Burglars broke through 24-hour security at New

Zealand Funds Management's offices in the ANZ Centre the weekend before

last. They stole computer tapes with clients' names, addresses, bank

account numbers, how much they had invested, as well as financial

advisers' computer passwords.

NZ Funds Management has about 25 000 clients throughout New Zealand, with about NZD 1.6 billion (about UDS 670 million) invested. The high-rise centre has swipe-card access, video security cameras, and security guards 24 hours a day, but the burglars got in at 4am the Saturday before last. They got away with computer taps holding the client information. Only one office was broken into and only the computer tapes stolen. Left behind were laptop computers and other equipment. ---NZPA [Source: \*Otago Daily Times\*, 26 Nov 2001, p. 28]

Strong cryptography wouldn't have helped. Completely avoiding the use of virus-friendly software wouldn't have helped. As for physical security, they had it. And the information was stolen anyway. Without knowing anything about the people involved, or having any expertise beyond that common to all readers of detective stories, I must say that it looks uncommonly like an insider job.

The distributed techniques that have been worked out in response to the Napster case, could they help to protect against loss of records like this? But wouldn't having businesses distributed their data over thousands of other business's machines create RISKS of its own?

---

**✶ Calif info: Ask and you shall be removed ... but you've got to ask**

"NewsScan" <newsscan@newsscan.com>

*Fri, 30 Nov 2001 09:05:04 -0700*

Responding to complaints by consumers and privacy advocates who protested California's legal sale to the Web genealogy company RootsWeb.com of public information containing such personal data as people's birth dates and their mothers' maiden names, the company now says it will remove from its Web site the names of anyone who makes a specific request. A spokesman for the company said: "The mission of our company is to create places to help people reconnect with their families. We're not in any way doing anything except helping our customers and if a customer is concerned about it, it doesn't do any good to leave them up on the site." A legal council for the Electronic Privacy Information Center says that California's sale of data to the genealogy Web site "a situation where all the residents of California have now been exposed to a new risk of identity theft." [\*San Jose Mercury News 30 Nov 2001\*; NewsScan Daily, 30 Nov 2001]

<http://www.siliconvalley.com/docs/news/svfront/priv113001.htm>

[The birth records of more than 24 million Californians are involved. PGN]

---

## **⚡ "Light turnout" for election**

grr/sll <grrhodes@nauticom.net>

*Wed, 28 Nov 2001 16:45:55 -0500*

During the recent election (November) here, a power outage occurred during voting hours. It lasted several hours and affected an estimated 10,000 people in portions of northern Allegheny and adjacent counties (north of Pittsburgh, Pennsylvania, USA). Initial news reports noted concerns that the voting machines would not work without electricity. From what I've gathered, most of the machines were lever-style machines, and had a provision for manual power (i.e., a crank) to tally the votes and reset the levers after each voter.

But what would have happened if they had used computer or other electronic voting, or another machine that required electricity to work? It seems dubious that backup power systems (15+ hour capacity) would be provided for all the polling places. How would the election process be affected, and when would the "powerless" voters vote? Would the election results be held up for this? -- it seems that they would have to be. [Of course, no one can predict how this might affect, or not, any election in Florida. ;-)]

Coincidentally, it was a relatively "minor" election, with few major offices or issues at stake, so fewer voters than normal showed up to vote. Around here, that's called a "light turnout" of voters. But, as they read their copy describing the local voting predictions and the "light turnout," not one of the newscasters gave any sign that they understood the pun.

[And yet it is not difficult to have a shocking experience even when there

is no electricity! PGN]

---

## ✶ The destruction of 7 WTC

"Jacob Harris" <jacob.harris@alacra.com>

*Fri, 30 Nov 2001 10:06:24 -0500*

While we know all too well about the horrific destruction of the two main towers at the World Trade Center (1 and 2 WTC), not as many people are aware of the destruction of nearby 7 WTC nearby approximately 8 hours after the initial impact. While the building sustained structural damage from falling debris and the collapse of the main towers, it was also consumed by a raging fire that seems to have caused similar catastrophic structural failure. This article in *\*The New York Times\** <<http://www.nytimes.com/2001/11/29/nyregion/29TOWE.html>> (reg required) indicates that a likely cause of that fire was the approximately 42,000 gallons of diesel fuel (6K gallons on the seventh floor, 36K in the basement) stored in the building to power backup generators for the City's emergency command center located there. This fuel was apparently ignited (the fireproof tanks may have been ruptured by debris) and burned intensely in the building's core to cause the collapse. Of course, the aforementioned emergency center was unusable in this emergency, and the city was left scrambling to setup another facility for emergency coordination (City Hall

was too close to the accident site). Finally, according to an earlier NY Times article, this building also housed a regional CIA office whose destruction has hindered some intelligence and investigation efforts.

As has been noted previously, the 9/11 disaster has illustrated all sorts of risks that are gruesome to contemplate. In hindsight, locating the emergency coordination center at the location of a potential emergency was unfortunate, and the lack of a backup emergency coordination center compounded the problem. And it is ironic how preparedness for one common emergency (power outages) can create a vulnerability in itself. I'm sure there are a lot more sites looking more nervously at their backup fuel supplies these days.

---

## **✶ Connecticut Attorney General website wants Microsoft browsers?**

"Ed Ravin" <eravin@panix.com>  
*Wed, 28 Nov 2001 12:48:47 -0500 (EST)*

A friend just sent me a pointer to the announcement that the Connecticut Attorney General is opposing the Microsoft settlement. The URL for the announcement is:

<http://www.cslib.org/attygenl/mainlinks/linkindex11.htm>

When I surf over there with my Opera 5.0 or Netscape 4.77 browser running on

Linux, I get this error page:

This site requires JavaScript to be enabled.

The Web browser that you are using does not have JavaScript enabled, or is not a JavaScript-capable browser. [...]

The link to "upgrade your browser", naturally, suggests that I use Microsoft Internet Explorer or Netscape.

(1) I shouldn't have to enable JavaScript just to read your press releases, but more importantly, (2) both browsers that I tried, Netscape 4.77 and Opera 5.0, running under Linux, have JavaScript enabled already. Something is clearly broken here.

It is ironic that the Attorney General's attempts to fight Microsoft's market dominance are undermined by a Web site that insists that its users switch to Web browser software provided by the market leaders. Talk about anti-competitive forces!

Ed Ravin <eravin@panix.com>

---

## **⚡ How to crash a phone by SMS**

Monty Solomon <monty@roscom.com>

*Wed, 28 Nov 2001 22:22:08 -0500*

How to crash a phone by SMS

By John Leyden

Posted: 28/11/2001 at 18:20 GMT

So now you can send an SMS and crash a mobile phone, so that the

user is locked out. Job de Haas, a security researcher at ITSX, has adapted a program called sms\_client, which sends an SMS message from an Internet-connected PC, in which the User Data Header is broken.

During a presentation during the Black Hat conference last week, he demonstrated how a malformed message crashes a Nokia 6210 phone on its receipt. Once the message is received it is impossible to turn on an infected phone again. ...

<http://www.theregister.co.uk/content/55/23080.html>

---

## **✶ The Web Never Forgets**

Monty Solomon <monty@roscom.com>

*Wed, 28 Nov 2001 22:21:33 -0500*

The Web Never Forgets, David Colker, Los Angeles Times, 27 Nov 2001

Government agencies have tried to remove sensitive information, only to discover that copies have proliferated and they're virtually impossible to eradicate. Within days of the 11 Sep attacks, the federal Agency for Toxic Substances and Disease Registry rushed to pull a suddenly sensitive report from its Web site titled "Industrial Chemicals and Terrorism." The agency eliminated all traces of the document and its description of sources for home-brew nerve gases and improvised explosives. But on the World Wide Web,

almost nothing truly dies. [...]

<http://www.latimes.com/news/printedition/la-000094419nov27.story>

---

## **✶ Risks of computer security education**

David Friedman <dkf5k@virginia.edu>

*Fri, 30 Nov 2001 13:29:06 -0500*

When Gary McGraw gave a talk to our Cryptology/Computer Security class at University of Virginia, one of the things he mentioned is that the "bad guys are a lot better at sharing than the good guys."

On Monday we had project presentations, and a group of students told the class how to exploit a serious security vulnerability present on any of the Lab PCs on grounds. The students had not told the system administrators of the machines about the vulnerability.

The RISK of educating people about computer security is nobody knows how the people getting educated are going to use their knowledge.

In this case I don't think my fellow students were acting maliciously. They simply didn't expect anybody to use the knowledge to do damage. It was a case of the "good guys" not sharing.

David Friedman

---

## **✶ Re: Let's get really paranoid about e-mail and spam (Hurst, [R 2178](#))**

"Walter Dnes" <waltdnes@waltdnes.org>

*Fri, 23 Nov 2001 23:21:14 -0500*

The general risk here is the use of software in conditions it was never designed to be run under. SMTP (\*SIMPLE\* Mail Transfer Protocol) is called that for a reason. It was designed to be run in a trusted environment -- i.e., for communications between researchers, professors, and military people who had sufficient security clearance to be allowed onto the ARPANET in the first place. It was never designed to thwart misdirection and forgeries by sleazy scammers, i.e. no built-in authentication. Servers were few and far between, run by a small community of administrators who probably knew each other on a first-name basis.

There is a spammer sub-culture (I use the term "culture" rather loosely) and also an anti-spammer culture, which are visible on various spam-fighting forums/ mailing-lists. What you see here is probably the result of a "dictionary attack". The following description is a simplification, and is not 100% technically exact. A service paid for or run by spammers will set up a script to probe an ISP's smtp server.

- if the smtp server supports the EXPN and/or VRFY commands an effective procedure is to establish an smtp connection to "smtp.example.com". Then run those commands inputting addresses like aaaaaaaa@example.

com,

aaaaaaab@example.com, aaaaaaac@example.com, etc, etc. A smarter script

will use a dictionary of common names to increase the percentage of hits.

The server will obligingly tell the connecting end which addresses are

for real, and which are invalid.

- if the smtp server has EXPN/VERFY disabled, another approach is to

run a bogus mass-mailing. Each e-mail transaction starts the process and gets as far as supplying the "To:" address. If the

receiving smtp server rejects an address, it's obviously invalid.

If the smtp server responds OK, then the address is valid. The

script will abort and tear down the e-mail transmission in that

case, and get on with testing the next e-mail address.

With today's fast computers and broadband, the above is feasible.

Spammers forge return addresses. This prevents the originating machine from getting e-mail-bombed if several percent of a multi-million spam run are

invalid addresses, or the targets' ISPs have spam-blocking of some sort. At

first spammers put in gobbledygook into the return address.

Then ISP's

started refusing e-mail from domains that didn't exist (this is a quick

lookup against DNS). So spammers resorted to forging random email addresses

at valid domains. Occasionally, the forgery will be identical to a valid

e-mail address, and innocent people get the bounces.

> how on earth did the spammers "harvest" my specific MyRealBox account name

They probably used some "common.name@myrealmailbox.com" forgery, as mentioned above.

> (And are there any steps one can take to prevent it from happening again?)

Not very much. You could try a long gobbledygook-type e-mail address that is less vulnerable (nothing is invulnerable) to a dictionary attack that is biased to common names. The disadvantage is that your friends and business associates will have problems remembering your kjgrhjkfdh@example.com e-mail address.

> This also brings to mind the risk of using a "free" Internet e-mail

Actually, the risk is in signing up with any ISP/e-mail-service with millions of valid e-mail addresses where a dictionary attack will return a lot of hits. You're less likely to run into this on a smaller ISP.

Walter Dnes <waltdnes@waltdnes.org>

[SMTP EXPN also noted by Doug Sojourner, in very similar discussion. PGN]

---

**✉ Re: Let's get really paranoid about e-mail and spam (Hurst, [R 21 78](#))**

Jason Bennett <jasonab@acm.org>  
*Tue, 27 Nov 2001 02:21:55 -0500*

Allan's story about all his mailboxes getting hit with spam doesn't really surprise me. I strongly suspect that he was the victim of a dictionary attack (mentioned several times before in RISKS).

When I started a new job last year, my e-mail account was set up a couple of weeks before I started (I had to move several hundred miles for this job). When I did start, I found my mailbox containing several hundred spams! I had, unfortunately in this case, been assigned the e-mail address of jason@domain. It was pretty much a given that most domains would contain an address of "jason," and so I got caught in those spam dragnets. Whenever I would go on vacation, I would come back to several hundred junk messages.

Lesson? An easier e-mail address is easier for everyone.

Jason Bennett, jasonab@acm.org

[We had a lot of e-mail on this topic. PGN]

---

## ✶ Re: Risks of the space in Unix filenames (Spinellis, [R 21 79](#))

David A. Moon <david-moon@rcn.com>  
28 Nov 2001 08:50:33 -0800

Some of Mr. Spinellis' suggested fixes won't help when a quote character appears in a filename.

This "requoting problem" has been known since before Unix even existed, at

least within the Multics community. I remember encountering it myself in 1971 or 1972 in the exec\_com facility of Multics.

The root cause and the real source of the risk here is the attempt to use an interactive command language as a programming language. It's evidently a very seductive temptation, since the mistake has been repeated many times by many people, but in the end that approach just can't work. A programming language needs a syntax and semantics that don't confuse the data being processed with the program doing the processing.

---

## **⚡ Re: Risks of the space character in Unix filenames**

"Dr Richard A. O'Keefe" <ok@cs.otago.ac.nz>

*Thu, 29 Nov 2001 14:15:21 +1300*

I can't be the only RISKS reader with an MPW documentation set, can I?

Apple has had a UNIX-like shell for many years. Let me quote page 3-18 of "Introduction to MPW" (that's \*M\*acintosh Programmer's Workshop):

### QUOTE PARAMETERS THAT CONTAIN SPACES

In general, when a parameter contains a space, you must enclose it in quotation marks so that the MPW Shell recognizes it as a single parameter.

and page 3-19:

### QUOTING RULE #1

Place quotation marks around parameters that contain spaces.

While UNIX may (perhaps!) have been new to Apple programmers, the need for quoting parameters that contain spaces certainly wasn't.

---

## 🔥 REVIEW: "Hackers Beware", Eric Cole

Rob Slade <rslade@sprint.ca>

Mon, 26 Nov 2001 07:59:28 -0800

BKHKRBWR.RVW 20010829

"Hackers Beware", Eric Cole, 2001, 0-7357-1009-0,

U\$45.00/C\$67.95/UK#34.99

%A Eric Cole www.securityhaven.com eric@securityhaven.com

%C 201 W. 103rd Street, Indianapolis, IN 46290

%D 2002

%G 0-7357-1009-0

%I Macmillan Computer Publishing (MCP)

%O U\$45.00/C\$67.95/UK#34.99 800-858-7674 317-581-3743 info@mcp.com

%P 778 p.

%T "Hackers Beware: Defending Your Network from the Wiley Hacker"

It is difficult to maintain confidence in a book that, within six sentences of the opening of the first chapter, misspells the word "brakes." We are told that two developmental editors, two copy editors, two proofreaders, and no less than five technical reviewers had at this work. Did any of them pay attention to what they were reading?

Chapter one basically states that dangers are out there, security is bad, and companies should be concentrating on prevention, detection, and

education. Cole also nudges at the "hacking for protection" theory, without ever really examining it. A brief but reasonable list of security breaking activities is given in chapter two. Various steps and tools involved in gathering information about a network connected to the Internet are described in chapter three. Unfortunately, this explanation, while helpful to a potential attacker, has no utility for the defender: almost all of the data discussed must be publicly available for the network to function, and so there are no means of blocking this level of access. Spoofing, or masquerading, is dealt with in chapter four, but again, while some protective measures are provided, much more time is spent on the disease than the cure. After twenty six pages of telling you how to hijack sessions, including the best programs to use and how to operate them, chapter five gives us two pages of simplistic advice (avoid remote connections) on protection. Chapter six lists a number of common denial of service attacks and, while it does devote a lot of ink to describing the exploits, the material is reasonably balanced, and the suggested defensive measures realistic. Chapter seven requires almost forty pages to tell us that buffer overflows are not good, and you should apply software patches. Password security is very important, but the material in chapter eight is vague, disorganized, and has relatively little to say about good password choice. (Chapters nine and ten describe some NT and UNIX password cracking programs.) The examination of background fundamentals of NT, in

chapter

eleven, is a terse and unfocused grab bag of information. The analysis It would be of little help in explaining the specific attack programs listed in chapter twelve, a number of which rely on particular applications. The same relation is true of chapters thirteen and fourteen, relating to UNIX. A number of backdoor and remote access trojan programs are described in chapter fifteen. Chapter sixteen discusses log files, and lists some programs for generating spurious network traffic in order to hide attacks. Some random exploits are listed in chapter seventeen, and a few more in eighteen. An attempt is made to combine various attacks into scenarios, in chapter nineteen, but these do not add anything to the material already provided. Chapter twenty is the usual vague look to the future.

This book takes the all-too-common approach of assuming that teaching you how to break into systems will help you to protect them. The work also amply demonstrates the fallacy of that argument. While the harried systems administrator spends several hours coming to grips with the minutiae of the attacks described, the vast majority of the exploits listed can be countered simply by ensuring that software patches are up to date. In addition, while dozens of loopholes are listed in these pages, thousands more exist that are not covered. The material contained in these pages may be entertaining, but it is of far more use to the attacker than to the defender. This would be upsetting, were it not for the fact that most of the exploits described are

old and not likely to remain unpatched if administrators are keeping up to date. (Of course, many small outfits can't commit a lot of resources to keeping up to date ...)

For security specialists, this volume provides nothing that can't be found elsewhere. For non-specialists, it fails to supply a security framework and strategy within which to work.

copyright Robert M. Slade, 2001    BKHKRBWR.RVW    20010829

As usual, a draft has been sent to the author. He has requested that this response be included, unedited:

Robert:

First allow me to say thank you for taking the time to review the book as criticisms are as crucial as praise. We take your feedback seriously. That being said, let me see if I might speak to some of your discussions on "Hackers Beware".

When you buy "Hackers Beware", you buy it for the technical content. While we maintain that this faction of the book is air-tight and well-supported, we also admit that we could and should have done a better job with edits on spelling and grammar. While we admit that shortcoming, we also ask that you look at the eleven reviews posted on Amazon, praising the technical content of my book and earning it FIVE- STAR rating.

The book starts opens with some introductory material but does that for a reason. Much of the security information that companies need to protect

their site is straightforward. Yet companies systems are still hacked into with a growing frequency because they fail to understand how to build a proper defense. So my book aims to ensure that everyone is well, if not over-educated on DEFENSE.

There are many books on hacking but what makes this book different is its emphasis on defense. Yes, you need to understand how the enemy breaks into systems, so you can build better defenses. Every section has an area on how to defend against a certain type of attack. So I am not sure how a review can say that defense is not covered when that is the thrust of this book. There are plenty of books that show you how to break in. This book clearly and explicitly explains the properties of a strong defense.

Thanks for letting me write a response. Eric

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 21: Issue 81**

**Friday 7 December 2001**

## Contents

- [Trader's error causes multi million-dollar loss](#)  
[George C. Kaplan](#)
- [Security hole at WorldCom left internal computer networks at risk](#)  
[PGN](#)
- [Judge ordered hack of Interior Department trust fund system](#)  
[James H. Paul](#)
- [NatWest bank turns debits into credits](#)  
[Bob Buxton](#)
- [Cops get speeding tickets from cameras](#)  
[Monty Solomon](#)
- [Gwinnett County GA keeps prison inmates list online](#)  
[Nick Brown](#)
- ["Late-night" Internet-porno-ban](#)  
[Debora Weber-Wulff](#)
- [Optimizations at kiosks can be costly](#)  
[Seth Arnold](#)
- [Grocery self-checkout risks](#)  
[Scott Nicol](#)
- [Swedish police reportedly doctor video evidence, admit it](#)  
[Jerry via Declan McCullagh](#)

[Ulf Lindqvist](#)

● [E-voting and international law](#)

[Lucas B. Kruijswijk](#)

● [Re: "Light turnout" for election](#)

[Andrew Fleisher](#)

● [Re: Connecticut AG website wants Microsoft ...](#)

[Roland Roberts](#)

[Nathan Sidwell](#)

● [Re: PLEASE REMOVE me from the CAL database](#)

[RootsWeb HelpDesk](#)

● [Re: REVIEW: "Hackers Beware", Eric Cole](#)

[Mark Brader](#)

● [Info on RISKS \(comp.risks\)](#)

---

## ✶ **Trader's error causes multi million-dollar loss**

"George C. Kaplan" <gckaplan@ack.berkeley.edu>

*Tue, 04 Dec 2001 08:19:18 -0800*

An article in the *\*Wall Street Journal\** on 3 Dec 2001 describes how a simple data-entry error could end up costing UBS Warburg up to \$100 million:

Dentsu Inc., one of the world's biggest advertising companies, was making

its trading debut Friday on the Tokyo Stock Exchange after completing one

of the year's biggest initial public offerings -- a deal arranged by UBS

Warburg, a unit of Switzerland's UBS AG, ...

Before the Tokyo market opened Friday, a UBS Warburg trader entered what

was intended to be an order to sell 16 Dentsu shares at 610,000 yen

(\$4,924.53) each or above. Instead, the trader keyed in an

order to sell

610,000 Dentsu shares at 16 yen apiece ...

The order was canceled by 9:02 AM, but not before 64,915 shares, almost half

of the 135,000 shares in the IPO, had been sold. The price of Dentsu

shares, which had been bid up to 600,00 yen before the market opened, fell

to 405,000 yen. Now, UBS Warburg is obligated to deliver the shares it

sold, and will have to buy them on the open market.

The article doesn't say anything about sanity checks in UBS's trading

software. These have their own risks, of course, but you'd think that an

error of 4 orders of magnitude in the selling price would at least merit an

"Are you sure?" before the order went through.

Once again, we see how computers let people make really big mistakes quickly.

George C. Kaplan. Communication & Network Services, University of California

at Berkeley 1-510-643-0496 gckaplan@ack.berkeley.edu

---

## **✶ Security hole at WorldCom left internal computer networks at risk**

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

*Thu, 6 Dec 2001 10:16:14 PST*

A security hole at WorldCom Inc. left internal networks at several of the

nation's top companies (e.g., AOL Time Warner, Bank of America, CitiCorp,

News Corp., JP Morgan, McDonald's Corp., Sun Microsystems) open to hackers. Adrian Lamo, a consultant in San Francisco, worked with WorldCom to fix the months-old problem over the weekend. There is no evidence that the security hole had been exploited, although it was possible to reconfigure or shut down corporate networks. Lamo: ``These networks were never designed to be connected to the Internet, They were private circuits running between locations.''

[Source: eponymous AP item, 05 Dec 2001, PGN-ed]  
<http://www.siliconvalley.com/docs/news/tech/080991.htm>

---

## ✶ Judge ordered hack of Interior Department trust fund system

"James H. Paul" <jpaul@Capaccess.org>

*Wed, 05 Dec 2001 15:17:56 -0500*

In an extraordinary step approved by a federal judge, a computer expert hacked his way into a government-run, Denver-based financial system last summer, created a false account and later altered yet another account. All this happened without the hacker being detected. Those steps, endorsed by U.S. District Judge Royce C. Lamberth in advance, were revealed Tuesday as part of a court case involving the Interior Department's handling of more than 300,000 trust accounts it is supposed to manage for American Indians. A court-appointed master said the ease with which the government's computer system could be penetrated was "deplorable and inexcusable." In a report

ordered released by Lamberth, the special master, Alan Balaran,  
called on  
the judge to seize control of the system. [Source: Court-  
appointed hacker  
altered Indian accounts, by Bill McAllister  
<bmcallister@denverpost.com>,  
\*Denver Post\* Washington Bureau Chief, 5 Dec 2001  
(<http://www.denverpost.com/Stories/0,1002,53%257E254976,00.html>); PGN-ed

[The DoI Web site is now OFF THE NET. PGN]

---

## ⚡ NatWest bank turns debits into credits

Bob Buxton <bob\_buxton@uk.ibm.com>

*Mon, 03 Dec 2001 11:35:36 +0000*

NatWest Bank (UK) online banking service offers the ability to  
download bank  
statement information into Quicken and Microsoft Money on your  
PC and until  
recently this worked correctly.

Previously you could choose to download all of your transactions  
from  
multiple accounts in a single download, now you have to download  
each  
account separately which takes much longer - especially since  
when using  
Netscape it forces you to go through the long winded logon  
procedure each  
time.

But the real problem is that the information that you download  
into Quicken  
or Microsoft money in the .OFX file format is plain wrong. It  
shows  
standing orders out of my account as credits into the account!

This of course results in the account balance appearing to be much higher than it should be and as a result I went overdrawn before I realized what was going on.

The NatWest help desk acknowledge that this is a known problem but don't know when the problem will be fixed and have done nothing to warn customers or disable the function from the web site.

---

## ✶ Cops get speeding tickets from cameras

Monty Solomon <monty@roscom.com>

*Sat, 1 Dec 2001 16:10:41 -0500*

Cops get speeding tickets from cameras

By Brian DeBose, *\*The Washington Times\**, 1 Dec 2001

Some D.C. police officers say they are slowing their response to emergencies because photo-radar cameras are ticketing them for speeding on Code One calls, and they are being forced to pay the fines.

At least three D.C. police officers told *The Washington Times* they were caught by the cameras and ticketed while on official police business. They said they and other officers have been forced to pay the fines, and are now on edge about speeding to a crime scene and running red lights in emergencies. Like area motorists, they have little chance of getting a reprieve from the D.C. Bureau of Traffic Adjudication without evidence to present in their defense. ...

Some officers have paid so many tickets that they are no longer speeding or running red lights to get to their dispatched calls even in emergency situations, Sgt. Neill said. ...

<http://www.washtimes.com/metro/20011129-13345237.htm>

---

## **✶ Gwinnett County GA keeps prison inmates list online**

Nick Brown <Nick.BROWN@coe.int>

*Thu, 6 Dec 2001 13:48:45 +0100*

As reported at the excellent [www.cruel.com](http://www.cruel.com):

Wondering what happened to that acquaintance from Gwinnett County, Georgia, from whom you haven't heard in a while ? Try <http://www.gwinnettcountysheriff.com/Docket%20Book.htm>.

The RISKS are many and varied, but to get you started, click on the link to see the list of charges against any inmate, at the end of which you find:

"If you have reason to believe this information is inaccurate, you may submit a request for review to:

Gwinnett County Sheriff's Department  
Records Section  
2900 University Parkway  
Lawrenceville, Georgia 20043"

No indication is given of how long it takes between one's (postal) application to have incorrect details removed, and the update to

the Web  
site, but presumably the interval can be reduced if your lawyer  
can spell  
"defamation".

---

## 🔥 "Late-night" Internet-porno-ban

Debora Weber-Wulff <weberwu@fhtw-berlin.de>  
*Wed, 05 Dec 2001 15:02:30 +0100*

German officials are apparently attempting to prove that the  
PISA results  
(Germany is pretty much at the bottom of the pack in regards to  
education  
world-wide) are true and anyone, no matter how ignorant, can be  
a politician  
in Germany:

The German Federal Government and the State governments have  
agreed to new  
measures for protecting youth from pornography on the Internet:  
according to  
the "Financial Times Deutschland" ([http://www.ftd.de/pw/de/  
FTDPRAR3MUC.html](http://www.ftd.de/pw/de/FTDPRAR3MUC.html))  
all such content is banned from 11 p.m. until 6 a.m.

No, this is not April Fools' Day. Really. The German  
government seems to  
think that when it is 11 p.m. in Germany, it is 11 p.m.  
everywhere else. And  
that all those XXX folks on the Internet will happily turn off  
the sleaze  
during the German day when the kiddies are awake.

This has of course caused an uproar amongst those in the know.  
Spiegel-on-line wrote an open letter to the guy in charge of  
publishing this  
nonsense, Frank-Walter Steinmeier

<http://www.spiegel.de/netzwelt/politik/0,1518,170361,00.html>

[The sarcastic wit in the letter may not make it through Babelfish intact, but it is quite funny]

What a sorry state of affairs. The risks posed by ignorant politicians may yet be far more dangerous than the odd virus and software mistake.....

Prof. Dr. Debora Weber-Wulff, FHTW Berlin, Treskowallee 8, 10313 Berlin  
+49-30-5019-2320 <http://www.f4.fhtw-berlin.de/people/weberwu/>

---

## ✂ Optimizations at kiosks can be costly

Seth Arnold <sarnold@marcelothewonderpenguin.com>  
*Tue, 27 Nov 2001 18:28:30 -0800*

Like Richard Akerman and Geoffrey Brent, an automated vending machine's failure mode caught me by surprise. However, what I interpreted as a failure mode may just be an optimization:

When purchasing a bus pass from an automated credit-card kiosk, I was informed "Authorization Denied" after selecting the pass I wanted, so I took my card and walked away. A kind soul ran up to me, handing me my receipt. An unkind soul didn't bother to hand me my bus pass.

As far as I can figure, the Authorization Denied screen was probably the last screen displayed on an off-screen buffer -- upon switching the display to the previously off-screen buffer, the machine did not clear

the old  
screen. I imagine had I waited two more seconds, the machine  
would have  
informed me of the successful transaction.

While I can think of several technological solutions to this  
problem, I  
decided to do something more pragmatic: purchase my bus tickets  
from the  
human-operated vending station a few blocks away.

(And yes, several phone calls and two days later, my money was  
refunded to  
my card.)

---

## ✂ Grocery self-checkout risks

Scott Nicol <sbnicol@mindspring.com>

*Thu, 06 Dec 2001 00:37:22 -0500*

This past summer, two major grocery store chains in my city  
installed  
self-checkout lines. They are arranged in groups of four, with  
one cashier  
station supervising the group.

Credit-card purchases can be signed for at the self-check line  
(electronic  
pad), but sometimes the line's register will prompt you to go to  
the  
cashier's station to finish your transaction. In other words,  
credit-card  
transactions for 4 different stations are handled at one  
register.

On my August credit-card statement, I noticed two charges on the  
same day in  
the same store. To make a long story short, the charge was  
finally reversed

today. The "extra" charge was for the checkout line adjacent to the one I used, and was completed before my checkout was complete (it showed up first). The head cashier volunteered today that she had dealt with one other customer who had the same thing happen.

The only strange thing about the checkout was that, at the end of the transaction, I was prompted to swipe my card twice, then prompted to go to the cashier station to sign the receipt. Swiping a card twice isn't unusual - credit cards and credit-card readers aren't perfect. Having 4 different card readers connect to one cash register is. I assume, in this case, the system assigned the first swipe to the order from the adjacent line, and the second swipe to my order.

Scott Nicol <sbnicol@mindspring.com>

---

## **Swedish police reportedly doctor video evidence, admit it**

Declan McCullagh <declan@well.com>

*Sat, 01 Dec 2001 19:07:13 -0500*

Date: Sun, 2 Dec 2001 01:19:37 +0100

>From: jerry@xs4all.nl

To: <declan@well.com>

Subject: Swedish police files complaint against themselves

interesting article re Video Evidence in belgium newspaper;

[http://www.standaard.be/nieuws/buitenland/index.asp?](http://www.standaard.be/nieuws/buitenland/index.asp?doctype=detail.asp)

[doctype=detail.asp](http://www.standaard.be/nieuws/buitenland/index.asp?doctype=detail.asp)

&ArticleID=DST01122001\_034 (in Dutch)

re. [www.svt.se/granskning/reportage.asp?S=744&A=744](http://www.svt.se/granskning/reportage.asp?S=744&A=744)

(Swedish)

quick translation;

Swedish police filed a complaint against themselves after a Swedish TV show revealed that police used manipulated video footage as evidence.

The TV show Uppdrag Granskning [<http://www.svt.se/granskning/>] compared its own footage with the evidence used by the attorney general.

The comparison shows that images were swapped, sound was edited, and police brutality cut out. Scenes where 19 year old Hannes Westberg gets shot in the belly have been tampered with.

PS. The complaint is about copyrights and abuse of power. Jerry

POLITECH -- Declan McCullagh's politics and technology mailing list

You may redistribute this message freely if you include this notice.

Declan McCullagh's photographs are at <http://www.mccullagh.org/>

To subscribe to Politech: <http://www.politechbot.com/info/subscribe.html>

This message is archived at <http://www.politechbot.com/>

---

## **Swedish police reportedly doctor video evidence, admit it**

Ulf Lindqvist <[ulf@sdl.sri.com](mailto:ulf@sdl.sri.com)>

*Sun, 2 Dec 2001 21:38:01 -0800 (PST)*

This is in agreement with what I have read in Swedish media.  
What is

missing here is that the prosecutor's office has repeatedly tried to obtain raw film footage from TV stations, presumably to compare with the police videos, but they refused and the Supreme Court agreed with the media. Out of context, it sounds pretty nasty that a teenager was shot by police, but it is apparently proven that he was hurling 4x4x4 inch solid cubic pavement stones at an officer who was already badly wounded from previous stones, bleeding and semiconscious. The police, relatively inexperienced with riots, were armed with nightsticks and pistols only, nothing "in between" such as water cannons, teargas/pepper spray or rubber bullets.

---

## **✶ E-voting and international law**

"Lucas B. Kruijswijk" <L.B.Kruijswijk@inter.NL.net>

*Mon, 3 Dec 2001 00:18:25 +0100*

Many articles were posted about the risks of computers with elections. I wondered to which extend the national Constitutions and International Law protects the election process and reduces the risks. After some research I made the conclusion that some kinds of voting are indeed violating International Law. This means that there is a risk that a judge may forbid some kind of voting methods, making the investment worthless. I also asked my government (the Dutch government) to react on the issues which led to remarkable responses.

The Dutch government is investigating the possibilities of two new ways of voting. Voting at home with the use of the Internet and voting with a "voting pillar". The voting pillars can be placed in public areas. There are no officials nearby and the pillar is controlled remotely. The voter has to identify itself with an electronic card with biometric information (iris recognition).

Both ways of voting can not ensure that the voter is alone when he/she casts his/her vote. There are no technical solutions known that prevent that couples votes together at home. It might be possible to ensure this for a voting pillar, but with the different body sizes this is certainly not trivial. These limitations conflict with International Law.

First of all, there is article 21.3 of the Universal Declaration of Human Rights:

"The will of the people shall be the basis of the authority of government;  
this shall be expressed in periodic and genuine elections which shall be  
by universal and equal suffrage and shall be held by secret vote or by  
equivalent free voting procedures."

But more precise and more important is article 25.b of the International Covenant on Civil and Political Rights:

"To vote and to be elected at genuine periodic elections which shall be by  
universal and equal suffrage and shall be held by secret ballot,  
guaranteeing the free expression of the will of the electors."

When I read this article I conclude that the primary concern is the "free expression of the will". However, the only legal way to achieve this is by "secret ballot". So, if a government chooses a voting method where there is no indication that the free expression of will is compromised but where the vote is not secret, then this method is still not allowed to be used (obvious the reason for this is that it is very hard to determine whether a will is free or not).

The interpretation of "secret ballot" is now very important. Note that word 'ballot' refers to "voting balls" and not to the vote itself. There is a risk in translating this into another language, because a literal translation of 'ballot' might not exist. In such case a translation from "secret paper" is maybe better than a translation from "secret vote". According to the New Shorter Oxford Dictionary, the words "secret ballot" means "in which votes are cast in secret". So, the circumstances in which the vote is cast are important. If someone tells his/her vote afterwards, it is still a secret ballot (because the vote was \*cast\* in secret), but if two persons vote together with their personal computer, then it is not a secret ballot.

This does not necessarily imply that voting at home or with voting pillars are violating the Covenant. First of all if the voter is in such situation that there is no realistic possibility to ensure that he/she casts his/her vote in secret (for instance when he/she is abroad), then of course the

right to vote is more important than the secrecy of the vote. Second, the article in the Covenant does not specify the responsibilities of the States. You may argue that the secrecy of the vote is also the responsibility of the voter to some extent.

The Human Rights Committee made comments on this article. The Committee is allowed to make such comments under article 40 of the same Covenant. If a State did also sign the first optional protocols, then individuals (and they are admissible in this case) can ask the Committee for a judgment when domestic remedies are exhausted. So, the Committee is the highest court.

On paragraph 20 of the comments, the Committee says:

"States should take measures to guarantee the requirement of the secrecy of the vote during elections including absentee voting, where such a system exists."

The States are not fully responsible for the secrecy, but they are obliged to make effort to ensure the secrecy.

To my opinion the "voting pillars" violate the Covenant. The government can give the same service to the voter and ensuring the secrecy. It just adds a supervising official to the voting pillar. So, the government is not fulfilling its obligation of making this effort.

Voting at home via the Internet, is allowed for those people that live in remote areas or abroad. However, a judge might forbid it for people that live in urban areas where polling stations are not a practical

problem. A

judge is probably more willingness to listen when is realized that voting via the Internet will finally lead to the elimination of polling stations. In the Netherlands the introduction of voting machines led to a 10% reduction of polling stations, because of the expensive voting machines and budgets policies of the local governments (according to documents of the national government). When voting at home is possible, then less people will go to the polling stations, which result that polling stations are closed, which will result that more people will vote at home etc.

I have requested 'Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties' (the Ministry of the Interior or Home Department), to react on the matter of the Constitution and International Law in relation with the new ways of voting. The Ministry responded that the responsibility of the State for the secrecy of the vote is "facilitating". So, according to this principle the State is not responsible in anyway to ensure that the votes are cast in secret; it should only guarantee that the voters have the possibility to vote in secret. I think the Ministry is in error on this point. First of all, if that would be the case, then the Covenant should say something like "one has to right to vote in secret", but that are not the words of the Covenant. Second, it would mean that it is allowed to give the voter the option to make his/her vote with his/her name public on the Internet (the voter has still the possibility to vote in secret). I think one does not consider this as a proper way of voting.

In a new letter I explicitly asked the Ministry to react on the text of the Human Rights Committee. I also pointed on the inaccuracy of the Dutch translation on the words "secret ballot". Since I wrote this letter recently, I did not have a response yet.

Despite the fact that serious questions can be raised about the compatibility of the new voting methods with national Constitutions and International Law, the Ministry does not mention these in the official documents at all.

I hope they do a better job with security.

Lucas B. Kruijswijk <L.B.Kruijswijk@inter.nl.net>

---

**⚡ Re: "Light turnout" for election (Rhodes, [RISKS-21.80](#))**

Andrew Fleisher <andrew8@start.com.au>

*Mon, 03 Dec 2001 14:09:35 +1000*

[With respect to] power/phone outages and online voting, what about the case where there is localised damage to power or phone systems preventing people from using online voting systems in significant elections which are close? It makes the recent Florida debacle during the Presidential election seem simple.

---

**⚡ Re: Connecticut AG website wants Microsoft ... (Ravin, [RISKS-](#)**

## [21.80](#)

Roland Roberts <roland@astrofoto.org>

*03 Dec 2001 12:28:57 -0500*

I took a look at this with both Netscape 4.77 and Mozilla 0.95 (both on Linux) and it displayed fine. The only "functionality" provided by Javascript appears to be a pop-up that tells me the site is best viewed at 800x600 or 1024x768.

I think the real issue here is general stupidity: turning a "nice" feature (the pop-up about resolution) into an absolute requirement.

Roland B. Roberts, PhD, RL Enterprises, 76-15 113th Street, Apt 3B  
Forest Hills, NY 11375    roland@rlenter.com    roland@astrofoto.org

---

## **✶ Re: Connecticut AG website wants Microsoft ... (Ravin, [RISKS-21.80](#))**

Nathan Sidwell <nathan@acm.org>

*Mon, 03 Dec 2001 11:13:35 +0000*

I've noticed more and more of this kind of brokenness over the last 12 months. (This is with Netscape on Solaris or Linux.)

1) An Internet bank (which no longer has my custom), broke the 'print' capability of all but IE. And then failed to understand that (a) the Web != Microsoft, and (b) a standalone machine would not be connected

to the web.

2) A credit-card company had the same problem. It used to work, but back in May it broke. I reported the problem and nothing has happened since then.

3) Many Flash sites claim I have not got flash enabled. One of these has enough smarts to say something like 'You don't appear to have Flash, go <here> to get it or go <here> to continue, if you know our check bombed out'

Dr Nathan Sidwell :: Computer Science Department :: Bristol University  
nathan@acm.org <http://www.cs.bris.ac.uk/~nathan/> nathan@cs.bris.ac.uk

---

## **[Re: PLEASE REMOVE me from the CAL database \(RootsWeb, RISKS-21.80\)](#)**

RootsWeb HelpDesk <helpdesk-post@rootsweb.com>  
*Sat, 1 Dec 2001 13:35:12 -0700*

[This was the reply many of us received in response to requests to be removed from the RootsWeb database noted in [RISKS-21.80](#). Apparently quite a few RISKS readers made such requests! PGN]

A response to your Help Desk message, "PLEASE REMOVE me from the CAL database," of Saturday, 1 December 2001, at 12:52 p.m. follows [...]:

As some states have passed laws to make their records publicly available,

many of these records have been made searchable on RootsWeb.com for genealogical purposes. This data is a great asset to many individuals doing family history research.

In addition to our goal to provide outstanding genealogical resources to our users, MyFamily.com is very committed to the privacy of those using our services, whether on MyFamily.com, Ancestry.com or RootsWeb.com. For this reason we have removed the CA and TX birth records from our site.

---

## ✂ Re: REVIEW: "Hackers Beware", Eric Cole (Slade, [Risks-21.80](#))

Mark Brader <msb@vex.net>

Sat, 1 Dec 2001 20:57:46 +0000 (UTC)

> %T "Hackers Beware: Defending Your Network from the Wiley Hacker"  
> ... within [the first] six sentences , misspells the word "brakes."

It would be still more impressive if the title was misspelled [Wiley] as shown above. Or was that one the reviewer's error, perhaps induced by familiarity with books published by Wiley?

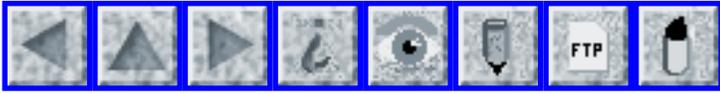
Mark Brader, Toronto, msb@vex.net

[Note: It is actually wrong [Wiley, and not too wily!] on the cover page

as shown on the Wiley Web site:

<http://images.amazon.com/images/P/0735710090.01.LZZZZZZZ.jpg>

The Wiley Coyote Editor must have been working overtime. 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 21: Issue 82**

**Friday 14 December 2001**

## Contents

- [Cisco accountant's fraud](#)  
[David Weitzel](#)
- ["The Missile Defense Hoax"](#)  
[Lauren Weinstein](#)
- [Military intelligence at its best?](#)  
[Terry Labach via Alan Wexelblat](#)
- [Office XP, Windows XP may send sensitive documents to Microsoft](#)  
[David Farber](#)
- [MS Word XP "autocorrects" my name](#)  
[Arnold Weissberg](#)
- [P3P, IE6 and Legal Liability](#)  
[Ben Wright](#)
- [SMS phone crash exploit a risk for older Nokias](#)  
[Monty Solomon](#)
- [Identity theft without prior knowledge of social security number](#)  
[Identity withheld by request](#)
- [FBI may not appreciate the risks with Carnivore sniffing E-Mail](#)  
[Fredric L. Rice](#)
- [Number takes prime position](#)  
[technews](#)

- [Radio-synchronised alarm clocks](#)  
[Jonathan D. Amery](#)
  - [Computer will drives 820 passengers at 68 mph](#)  
[Daniel Norton](#)
  - [Re: "Late-night" Internet-porno-ban](#)  
[Debora Weber-Wulff](#)
  - [Re: Risks of various characters in Unix filenames](#)  
[Duncan MacGregor](#)  
[Bennet S. Yee](#)
  - [NetSOL vs. PGP: Risks of a crypto company owning a registrar?](#)  
[R. A. Hettinga](#)
  - [Swedish police reportedly doctor video evidence, admit it](#)  
[Michael Walsh](#)
  - [Followup to: Savings Bank software upgrade goes awry](#)  
[Jonathan Kamens](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

## ✂ Cisco accountant's fraud

david weitzel <dweitzel@mitretek.org>

*Thu, 13 Dec 2001 17:35:39 -0500*

www.cybercrime.gov:

Former Cisco Systems, Inc. Accountants Sentenced for Unauthorized Access to Computer Systems to Illegally Issue Almost \$8 Million in Cisco

Stock to Themselves (November 26, 2001)

<[http://www.cybercrime.gov/Osowski\\_TangSent.htm](http://www.cybercrime.gov/Osowski_TangSent.htm)>

Press release excerpt:

Judge Whyte sentenced the defendants each to 34 months in federal prison, restitution of \$7,868,637, and a three year period of supervised release. The defendants will begin serving their sentences on January 8,

2002.

David S. Weitzel, M.S., J.D., Senior Principal, Mitretek Systems  
dweitzel@mitretek.org 1-703-610-2970

---

## ✶ "The Missile Defense Hoax"

Lauren Weinstein <lauren@vortex.com>  
*Thu, 13 Dec 2001 12:33:37 -0800 (PST)*

Greetings. The latest short "Fact Squad Radio" audio piece addresses the risks related to the U.S. withdrawal from the 1972 ABM treaty. It's called "The Missile Defense Hoax" and can be accessed via:  
<http://www.factsquad.org/radio>

Lauren Weinstein Tel: +1 (818) 225-2800  
lauren@pfir.org or lauren@vortex.com or lauren@privacyforum.org

---

## ✶ Military intelligence at its best? (Retitled)

<quotationoftheday\_request@yahoo.ca>  
*Tue, 11 Dec 2001 05:55:06 -0500*

Quote of the day for December 11, 2001:

"As a pilot, I can do everything perfectly with a perfect weapon system, and still cannot account for every weapon going exactly where it's supposed to go."

U.S. Rear Admiral John Stufflebeem redefines the word

"perfect".

Stufflebeem was responding to the deaths of three U.S. soldiers in

Afghanistan after yet another bomb went astray.

Submitted by: Terry Labach, Dec. 6, 2001

[Submitted to RISKS by Alan Wexelblat <wex@media.mit.edu>. PGN ]

---

## **Office XP, Windows XP may send sensitive documents to Microsoft**

David Farber <dave@farber.net>

*Fri, 07 Dec 2001 07:59:49 -0500*

PROBLEM: Microsoft Office XP and Internet Explorer version 5 and later are configured to request to send debugging information to Microsoft in the event of a program crash. The debugging information includes a memory dump which may contain all or part of the document being viewed or edited. This debug message potentially could contain sensitive, private information.

PLATFORM:

- \* Microsoft Office XP
- \* Microsoft Internet Explorer 5.0 and later
- \* Windows XP
- \* Microsoft has indicated that this will be a feature of all new Microsoft products

DAMAGE: Sensitive or private information could inadvertently be sent to Microsoft. Some simple testing of the feature found document information in

one message out of three. SOLUTION: Apply the registry changes listed in this bulletin to disable the automatic sending of debugging information. If you are working with sensitive information and a program asks to send debugging information to Microsoft, you should click Don't Send.

<http://www.ciac.org/ciac/bulletins/m-005.shtml>

---

## **⚡ MS Word XP "autocorrects" my name**

Arnold Weissberg <[aweissberg@mindspring.com](mailto:aweissberg@mindspring.com)>

*Thu, 06 Dec 2001 19:39:48 -0500*

I typed my last name into a document. I thought something funny had happened because it came out with one "s." I never misspell my last name.

There was a line under the "W". Holding the mouse on this line I got the following choices:

1. Change back to "Weissberg"
2. Stop Automatically Correcting "Weissberg"
3. Control AutoCorrect Options

Now this is, as my grandmother would have said, real chutzpah. Telling me

how to spell my own name! Talk about arrogance--what's next, "anglicizing"

it? Like, auto correcting it to "Whitehill?" And if I try to change it

back will it say, "I'm sorry, Arnold, I can't do that"? I think in this

little example we can learn a lot about Microsoft's corporate attitudes

toward the rest of the world--that is, no one is smart enough even to be

trusted to spell their own name right. Much less choose what software they'd like to use.

[Not much new, but just one more instance -- which is so often the case in the RISKS archives. PGN]

---

## ✶ P3P, IE6 and Legal Liability

Ben Wright <Ben\_Wright@compuserve.com>

*Mon, 10 Dec 2001 10:07:12 -0500*

Privacy filters in Microsoft's new Internet Explorer 6 pose for Web administrators an unexpected legal predicament.

The filters force administrators to post new privacy policies for their Web sites, coded in a technical language called P3P. The filters punish administrators who fail to publish properly coded P3P privacy policies by blocking or impeding their cookies.

The P3P coding language raises, for any corporation, government agency or other institution that uses it, a lawsuit danger. A privacy policy written in it exposes the organization to liability, with little or no escape.

A privacy policy, even one written in computer codes, can be legally enforceable like a contract. In lawsuits filed in 1999, plaintiffs forced US Bancorp to pay \$7.5 million for misstatements in a privacy policy posted on its Web site.

Web administrators face a dilemma. They want to satisfy IE 6's technical requirement for P3P codes, but they also want to sidestep liability. See Webservice Online Magazine article:

<http://webserver.cpg.com/news/6.12/n5.shtml>

One solution is to deploy dummy P3P codes, with an extra legal code that disavows any liability for the codes, as explained at <http://www.disavowp3p.com>.

P3P is the Platform for Privacy Preferences, developed under the sponsorship of a non-profit organization named the World Wide Web Consortium (also called W3C) <http://www.w3.org/p3p>, a coalition of industry and non-profit groups.

--Ben Wright [ben\\_wright@compuserve.com](mailto:ben_wright@compuserve.com)

---

## **✶ SMS phone crash exploit a risk for older Nokias**

"monty solomon" <[monty@roscom.com](mailto:monty@roscom.com)>

*Fri, 7 Dec 2001 14:25:15 -0500*

SMS phone crash exploit a risk for older Nokias, by John Leyden, 12 Jun 2001

Nokia has upgraded its phone software to guard against a security glitch that might allow a cracker to render a phone inoperable by sending a text message. However, older phones may still be vulnerable.

<http://www.theregister.co.uk/content/55/23232.html>

---

## **✶ Identity theft without prior knowledge of social security number**

Identity withheld by request <>

*13 Dec 2001*

A while back I had few occasions when I was asked for my social-security number by organizations I felt have no business knowing it (such as libraries, etc.). Following advice from the Usenet SSN FAQ, I asked why they wanted my SSN, quoted appropriate legislation, and was allowed to give "a different number" (which these organizations presumably want as a primary key for their databases or for similar procedural reasons).

Needless to say, I used a meaningless word for mother's maiden name and a made up birth date, one per organization.

When I have later requested my credit report, I discovered that these silly made up numbers appear on the report as "Other social security numbers used." Along with their respective mother maiden names and birth dates. Apparently, credit-reporting agencies aggressively merge records in their databases.

A risk? Surely. Consider the following scenario:

1. Identify target for identity theft by name (common names could work).

Use the phone book to learn the address of the person in question. This is all the information you need to know.

2. Apply for a credit card in the name of that person, using a made up SSN, mother's maiden name, and birth date. (It doesn't matter if the request for credit is approved; the information you submit will get reported to credit agencies and they will merge it into the database entry of the target person based on matching name and address. You now have information that's sufficient to ask for a credit report.)
3. Ask a credit reporting agency for "your" credit report. You should be able to do it through a Web interface. (If you had to give them a mailing address, you could have asked for the report to be mailed to a temporary Mail Boxes, Etc address or to somebody else's street address where the mailbox is accessible and you can get to it before the rightful owner does--for example, because you know the owner's work schedule.)
4. Examine the credit report. It has the target's actual ("primary") social security number and other information.
5. Having that, proceed with identity theft in any number of well-known ways.

I have a fairly uncommon name. Maybe the record merging algorithm will not actually work with common names. Does anybody know more about their actual merging algorithm?

## **✶ FBI may not appreciate the risks with Carnivore sniffing E-Mail**

"Fredric L. Rice" <frice@skeptictank.org>

*Wed, 05 Dec 2001 11:57:43*

Probably everyone who reads RISKS has read about the United States' law enforcement agencies wish to implement anti-terrorism measures which adversely impact people's privacy. As reported in Yahoo Magazine, November 2001, the FBI has been pushing to get its Carnivore package installed at major Internet Service Providers like AOL and EarthLink so that subscriber's inbound and outbound E-mail can be flagged and read by the FBI.

Before the terrorist attacks on New York, activists had been trying to disrupt Carnivore and like-minded software packages by stuffing their Web sites, E-Mail messages, Usenet postings, and mailing list messages with likely terms and phrases that would trigger collection by Carnivore so that some hapless FBI stooge has to spend half a minute apiece looking through tens out thousands of messages. By now, I'd expect, the FBI has tailored its implementations of Carnivore to detect such repeated, invariant attempts to choke off their software's usefulness but did the FBI really consider all of the risks of using Carnivore? I doubt that they did.

You know what happens next, humans being ornery and downright stupid. What happens next is that activists and idiots both will start farming AOL and EarthLink E-Mail addresses and software will be written to start spamming those hundreds of thousands of addresses with variant message

texts

containing all the likely terrorism-related keywords inserted  
Mad-Lib

fashion. Tens of thousands of people will get E-Mail messages  
with forged

return addresses containing Mad-Lib-like generated terrorist  
plans and

Carnivore will flag on them. Then when the subscriber who gets  
the spam

forwards it to both uce@fbi.gov and Norfolk@fbi.gov, Carnivore  
gets two more

hits. If the subscriber is stupid enough to reply to the E-Mail  
(and let's

face it: They're using AOL or EarthLink so you know they're not  
very bright)

and now Carnivore sees a bi-directional link.

The risks are plenty. How many people will the FBI take off of  
real

criminal investigations and put onto the project to monitor and  
review bogus

Carnivore hits? If they hire new people, who's going to pay for  
them? How

many people are going to be visited by the FBI because some  
idiot keeps

sending them terrorist attack plans? The biggest risk is  
obvious and I have

to wonder why nobody in the FBI seems worried about it: Real  
terrorists will

slip through Carnivores' filtration criteria simply because you  
damn well

know that activists and idiots will be the ones who get to  
decide what

Carnivore filters and what it hits on.

How will activists get to drive Carnivore? Every time someone  
gets

questioned by the FBI or finds out from their neighbors that  
they've been

investigated, the victim will report the fact on the Internet  
maybe even

posting the E-Mail they received that triggered the software,  
prompting

activists and idiots to adopt the terms and methodologies which worked,  
prompting the FBI to tailor Carnivores' filtration until the next time.

I can't see anything coming out of the struggle besides a pile of useless software running on ISP's servers fingering innocent people and failing to point at a single bad guy.

---

## ⚡ Number takes prime position

technews <technews@HQ.ACM.ORG>  
*Mon, 10 Dec 2001 16:28:41 -0500*

The largest prime number yet to be documented has been discovered by Michael Cameron, a participant in the Great Internet Mersenne Prime Search (GIMPS). The project, founded in 1996 by George Woltman, aims to uncover new Mersenne primes through distributed computing. ...  
4,053,946 digits:  $2^{(12,466,917)} - 1$ . ... 130,000 volunteer participants ...

ACM TechNews - Monday, December 10, 2001  
<http://www.acm.org/technews/articles/2001-3/1210m.html#item13>  
[See that site for subscriptions. PGN]

---

## ⚡ Radio-synchronised alarm clocks

"Jonathan D. Amery" <jdamery@chiark.greenend.org.uk>  
*Mon, 10 Dec 2001 00:38:21 +0000 (GMT)*

I own a radio synchronised alarm clock (a friend of mine also has one that displays the same symptom). When the batteries are running low it will display the time just fine, but when it tries to sound the alarm there is insufficient power and it resets itself. Since it is radio synchronised it then starts showing the correct time after a minute or two. As a result I oversleep and get to work late, but since I often don't notice the clock going off and wake up a few minutes later I don't know that this has happened, and it carries on like this for many days until I notice. If this was a normal battery operated clock I would be able to tell because the time had reset.

---

## **✂ Computer will drive 820 passengers at 68 mph**

Daniel Norton <danorton@suespammers.org>

*Mon, 10 Dec 2001 14:10:20 -0500*

Here are some technical specification on the planned JFK Airport AirTrain:

>From <http://www.kennedyairport.com/airtrain/projectframe.htm>

...

Train Consist                    1- to 4-car trainsets

...

Train Control                    Fully automated, 24 hour  
per day operation

...

Maximum Design Speed        110 km/h 68 mph

...

Capacity per Car,           71 standees + 26 seated = 97 total  
Passengers with Luggage

...

Capacity per Car,           179 standees + 26 seated = 205 total  
Passengers without Luggage

So that's up to 820 passengers at up to 68 mph (110 kmh) under automated control. That's per train and multiple trains are likely to be operating at the same time.

I think the RISKS are obvious to readers here, but I'd like to know if there are similar automated passenger systems elsewhere and what actual problems, if any, they have faced.

Daniel Norton, NYC

---

## ✶ Re: "Late-night" Internet-porno-ban ([RISKS-21.81](#))

Debora Weber-Wulff <weberwu@fhtw-berlin.de>  
*Mon, 10 Dec 2001 10:57:39 +0100*

Debora wrote:

> >all such content is banned from 11 p.m. until 6 a.m.

Nick Brown responded:

> Don't you mean "banned except from 11 p.m. to 6a.m."?

> Papier zufolge duerften nicht jugendfreie Inhalte "nur  
zwischen 23 Uhr und

> 6 Uhr verbreitet". Presumably that gives people the choice: a  
drink in an

> Autobahnraststatte (which is banned between 2300 and 0600, I think), or a  
> porno session on the Net.

> Either way it's very funny. We've been here before though, when Germany  
> tried to take xs4all.nl offline because one page which it hosted had  
> pro-Nazi propoganda.

They never learn, do they?

Prof. Dr. Debora Weber-Wulff, FHTW Berlin, 10313 Berlin +49-30-5019-2320  
weberwu@fhtw-berlin.de <http://www.f4.fhtw-berlin.de/people/weberwu/>

---

## **⚡ Re: Risks of various characters in Unix filenames (O'Keefe, [R 21 80](#))**

Duncan MacGregor <aa735@freenet.carleton.ca>  
*Sat, 1 Dec 2001 19:46:33 -0500 (EST)*

Unfortunately, there are two assumptions that fail when shifting from the old Mac OS to a UNIX-based system.

One of these is the meaning of the word "quote." Unfortunately, different dialects of English give it a different meaning. In British English, it means the single quote, but in North American English, it means the \*double\* quote-mark. Fortunately, the phrase 'quotation mark' is often understood to refer to the North American rather than the British convention, though I may be wrong on that point. [And yes, I deliberately alternated

between single  
and double quotes just to drive the point home.]

The other assumption that fails, however, is much harder to catch. In UNIX, the single and double quote mark apply different meanings to the string that is contained in it. The single quote means that the string is to be taken *\*strictly\** as is, with no translation of substrings that might match shell or environment variables. Use of the double quote, however, means that such a substitution should be done.

This means that, if you have a literal string that includes reversed (single) quotes or dollar [currency] signs, you had better use single quotes or apostrophes [inverted commas?] to demarcate it, or get a shell variable interpolated inside it. Contrarily, double-quotes are needed if you do want such a substitution [though you should use braces or "curly brackets" (i.e., { }) to contain the variable name itself, just in case].

As for languages such as Perl and Tcl, that's an even messier tangle, with yet other methods for quoting ... (where's that Excedrin bottle? :-).

Hoping I'm not misquoted ...

Duncan MacGregor | aa735@freenet.carleton.ca  
Also at: "<http://www.ncf.carleton.ca/~aa735/>";

---

**⚡ Re: Risks of various characters in Unix filenames (Spinellis, [R 21 79](#))**

Bennet S. Yee <bsy@play.ucsd.edu>

11 Dec 2001 01:46:29 -0800

There are several problems with this approach. first, a newline is also a valid character in a filename, not just spaces. so if i create a file named "foo\nbar" in a directory that also contains files "foo" and "bar", this script will not process "foo\nbar" and process both "foo" and "bar" twice. next, if the subtree rooted at "." contains many files, this command could cause the shell to fail in trying to run the "wc" command, since more than ARG\_MAX number of bytes in the arglist will cause execve(2) to fail with errno set to E2BIG.

Of course, the gnu find utils authors provided a way handled this properly:

```
$ find . -type f -print0 | xargs -0 wc -l
```

This relies on the fact that on all unix filesystems thus far, the null character is not a legal character in a filename component.

While I'm nit picking, earlier in the article, a recommendation was made for doing sh/bash/ksh loops as

```
for arg in "$@"
do
...
done
```

which is fine in modern shells but once upon a time failed in older shells when there are no arguments. the simpler way of

```
for arg
do
...
done
```

Works just fine in the special case of "for" loops and is shorter besides.

in older scripts you'll see `${1+"$@"}` instead of just `"$@"` in non-"for" loop

contexts, since it handles the no-arguments case properly. of course, most

modern shells (such as bash) handles the no-arguments case for `'"$@"'`

"properly", i.e., the commonly desired interpretation of expanding to

nothing instead of a single zero-length argument.

The Risks:

- \* not knowing the existing / known methods to solve various shell quoting problems lead to reinvention of the wheel;

- \* trying to outwit shell quoting rules without fully understanding them

leads to ever subtler bugs which, because they probably occur with a lower frequency, will be harder to find again;

- \* incompletely considered reinventions can cause harm, esp if eagerly

adopted by other non-wheel-reinventors when published in fora like comp.risks.

Oh, while kernighan and pike may have commented on `"$@"`, the reference read

like a misattribution. s.r.bourne had it in his unix 7th edition shell. i

have no idea whether s.r.bourne came up with the notation -- after realizing

the need for something like it -- himself or had it suggested to him by

others, but its invention significantly predates the K&P book.  
perhaps this  
is just the Risk of my reading the article too quickly the first  
time.

Bennet S. Yee, Dept of Comp Sci and Eng, 0114, UC San Diego, La  
Jolla, CA  
92093-0114 +1 858 534 4614 <http://www-cse.ucsd.edu/users/bsy/>

---

## ✶ NetSOL vs. PGP: Risks of a crypto company owning a registrar?

"R. A. Hettinga" <rahettinga@earthlink.net>

*Mon, 10 Dec 2001 12:19:05 -0500*

Last week, IBUC and Shipwright's upstream provider, kc-inc.net,  
changed its  
own upstream access to the net, using Network Solutions' PGP  
interface to  
change the DNS server IPs after the wires were pulled and the  
lights went  
on. After a week of NetSOL saying that every thing was okay, to  
repeatedly  
retry the changes, and wait for the system to catch up, they  
came back today  
saying that, in fact, PGP authentication to their domain name  
registration  
system was broken, it might be broken for a while, and could kc-  
inc.net  
please send a \*fax\* authorizing the change, and they would walk  
it, by hand,  
it through the configuration process. Of course, authentication  
methods were  
put in place to avoid manual processing, so this is rather  
amusing.

NetSOL, of course, is owned by Verisign these days, and Verisign  
is an  
offspring of RSA, so, given the extant bad blood between RSA and

the various iterations of PGP development, it's a pretty fair assumption that there's no real desire to use the SAIC-installed PGP domain-control request system at NetSOL anymore...

My question is, would DNSSEC fix this mess?

R. A. Hettinga, The Internet Bearer Underwriting Corporation  
44 Farquhar Street, Boston, MA 02131 USA <http://www.ibuc.com/>  
(Reply to rah@earthlink.net, of course, as shipwright.com is \*still\* down, because I can't change my InterNIC handle via email to fix it :-)...)

---

## **Swedish police reportedly doctor video evidence, admit it (R 21 81)**

Walsh Michael <michael.walsh@wmdata.fi>  
*Mon, 10 Dec 2001 08:59:16 +0200*

Both RISKS correspondents seem in their own ways to have seen this program in a different way to myself.

For me the key difference between the Police video used by the prosecutor and the amateur video used mainly (there were a couple of other sources) by Swedish TV in the Granskning program was that the amateur video was running the entire time and from above (corner building; third? floor). Thus you could see that whereas initially a few police were being chased by a large group of stick-wielding, stone-hurling "demonstrators" (also shown on the

police video), by the time the person in question had been shot a large number of police reinforcements had arrived and the large group of demonstrators had mostly fled.

In other words whereas the police video showed a few police running away from a mob and in the end defending themselves with a few bullets; the amateur video supported by a couple of other sources showed that at the time of the shooting of the demonstrator the police had the upper hand.

The amateur video did however also seem to show that the demonstrator who was shot had been throwing paving stones at the police throughout the entire action from close by and had treated the whole thing as a huge joke. If this is so (it "seemed" to be the same demonstrator), I suspect this finally got to them.

Mike Walsh, Helsinki, Finland

---

## **✶ Followup to: Savings Bank software upgrade goes awry ([RISKS-21.53](#))**

Jonathan Kamens <jik@kamens.brookline.ma.us>  
*Tue, 11 Dec 2001 15:31:04 -0500*

Some of you might recall the tale I told in [RISKS-21.53](#) (published 19 Jul 2001) of problems with my bank's upgrade of their computer systems in June. Unfortunately, although it's almost five months later, the

situation still  
hasn't improved.

The bank still hasn't acknowledged that most of the problems I reported haven't been fixed. Most significantly, they still haven't admitted that they miscalculated interest on some accounts during the month of June, explained how the error occurred, explained how many accounts were affected, or fixed the error in the affected accounts.

I finally gave up on waiting for them to do the right thing as a result of only my inquiries. I've therefore contacted the local newspapers, the Massachusetts Division of Banks, and the FDIC and asked them to investigate. I've also put the whole story on-line at <URL:[http://www.mit.edu/~jik/pfsb\\_problem/](http://www.mit.edu/~jik/pfsb_problem/)>.

If you are interested in continuing to follow this story, please periodically check the above URL for updates (or you can let me know you're interested and I'll send you E-mail when there's new news). I will refrain from submitting any further articles to RISKS about this unless either (a) the bank actually does something substantive to address the interest miscalculation or (b) they prove that I'm wrong about it, in which case I'll submit a retraction :-).

Jonathan Kamens



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 21: Issue 83**

**Weds 26 December 2001**

## Contents

- [Error at Board of Studies](#)  
[Pete Mellor](#)
- [Wiretapping equipment compromised: FBI, CALEA](#)  
[Michael E. Goldsby](#)
- [Security problems in Microsoft and Oracle software](#)  
[NewsScan](#)
- [Latest Windows versions vulnerable to unusually serious attacks](#)  
[Monty Solomon](#)
- [Software glitch grounds new Nikon camera - Tech News - CNET.com](#)  
[Craig Mautner](#)
- [Secure in, insecure out](#)  
[Jeremy Epstein](#)
- [Assume no safety ...](#)  
[Peter Houppermans](#)
- [Re: Identity theft without prior knowledge of SSN](#)  
[Brett Harmond](#)
- [Mersenne prime exponent wrong](#)  
[Ken Knowlton](#)
- [Re: Computer will drive 820 passengers at 68 mph](#)  
[Ian Entecott](#)

[Jonathan Thornburg](#)

[Curt Sampson](#)

[Jeff Jonas](#)

[Jacob Sparre Andersen](#)

[Anthony W. Youngman](#)

[Andrew Roberts](#)

[Jens Braband](#)

[Jerrold Leichter](#)

 [Info on RISKS \(comp.risks\)](#)

---

## Error at Board of Studies

Pete Mellor <pm@csr.city.ac.uk>

*Sat, 15 Dec 2001 15:26:41 +0000 (GMT)*

The following was sent to the Dean (Cc the School) by one Head of Department last Friday. I thought it might provide a little Christmas cheer!

```
> Please give my apologies to the Board for the error
> in my last report. I had written,
> "There should be a rewording of BSc CS's position .. "
>
> My spellchecker challenged "CS's". Unfortunately I
> clicked 'Replace' rather than 'Skip' without noticing.
> The default substitute for "CS's" is "Chihuahuas".
```

Peter Mellor, Centre for Software Reliability, City University,  
Northampton Square, London EC1V 0HB +44 (0)20 7040 8422 [NEW]

```
[The spelling checker must have been a little dogged in its
persistent challenging. But it would be even more delightful
if
a Chihuahuan with a BSc degree had applied for the position.
PGN]
```

## ⚡ Wiretapping equipment compromised: FBI, CALEA

"michael e. goldsby" <mike.goldsby@attbi.com>

Thu, 20 Dec 2001 00:59:00 +0000

A recent series of four newscasts on the Fox Network alleged that U. S. telephone call records have been falling into the hands of international organized crime. Call records allow traffic analysis but do not disclose the contents of the conversations.

However, the newscasts further alleged that the equipment used by the FBI to do the wiretaps authorized by the CALEA legislation (1994) has been compromised. It is said to contain back doors that allow unauthorized persons to obtain access to the contents of telephone conversations. The back doors were not put there by the FBI and are not under their control.

Partial transcripts of the newscasts are available at

<http://foxnews.com/story/0,2933,40684,00.html>

<http://foxnews.com/story/0,2933,40747,00.html>

<http://foxnews.com/story/0,2933,40824,00.html>

<http://foxnews.com/story/0,2933,40981,00.html>

The second newscast cites an example of a 1997 Los Angeles drug case in which access to telephone call records was used to "completely compromise the communications of the FBI, the Secret Service, the DEO [sic] and the LAPD. "

---

## **✦ Security problems in Microsoft and Oracle software**

"NewsScan" <newsscan@newsscan.com>

*Fri, 21 Dec 2001 08:47:58 -0700*

Two top companies have issued new statements acknowledging security flaws in their products: Microsoft (Windows XP) and Oracle (the 9i application server, which the company had insisted was "unbreakable." Resulting from a vulnerability called "buffer overflow," both problems could have allowed network vandals to take over a user's computer from a remote location. Microsoft and Oracle have released software patches to close the security holes, and a Microsoft executive says: "Although we've made significant strides in the quality of the software, the software is still being written by people and it's imperfect. There are mistakes. This is a mistake." (San Jose Mercury News 21 Dec 2001; NewsScan Daily, 21 December 2001) <http://www.siliconvalley.com/docs/news/svfront/secur122101.htm>

---

## **✦ Latest Windows versions vulnerable to unusually serious attacks**

Monty Solomon <monty@roscom.com>

*Fri, 21 Dec 2001 01:21:03 -0500*

Microsoft's newest version of Windows, billed as the most secure ever, contains several serious flaws that allow hackers to steal or destroy a victim's data files across the Internet or implant rogue

computer software.

... A Microsoft official acknowledged that the risk to consumers was unprecedented because the glitches allow hackers to seize control of all Windows XP operating system software without requiring a computer user to do anything except connect to the Internet. Microsoft made available on its Web site a free fix for both home and professional editions of Windows XP and forcefully urged consumers to install it immediately. ... Ted Bridis, Associated Press, 20 Dec 2001

<http://digitalmass.boston.com/news/2001/12/20/microsoft.html>

[The vulnerabilities involve the universal plug-and-play features, and

were discovered by a team at eEye Digital Security Inc. of Aliso Viejo,

Calif., led by Marc Maiffret. There were also subsequent reports that the

free fix was not adequate. By the way, the free fix can arrive automatically with "drizzle", which allows MS to upgrade for you. PGN

SAYS BEWARE OF MECHANISMS THAT OFFER AUTOMATIC UPGRADES, no matter how

convenient they may seem. The article also quotes Microsoft's departing

corporate security officer, Howard Schmidt, who is about to join Richard

Clarke in the White House, expressing frustration about continuing threats

from overflows. "I'm still amazed that we allow these things to occur."

PGN]

---

**Software glitch grounds new Nikon camera - Tech News - CNET.com**

"Mautner, Craig" <craig.mautner@windriver.com>

Thu, 20 Dec 2001 15:29:22 -0800

From the article

[http://news.cnet.com/news/0-1006-200-8246450.html  
?tag=pt.msnbc.feed..ne\\_8246450:](http://news.cnet.com/news/0-1006-200-8246450.html?tag=pt.msnbc.feed..ne_8246450)

"...Given certain circumstances, the glitch can come into play if a person switches on the camera without first removing the lens cap. Depending on what position the zoom lens was in when the camera was last used, the lens cap will block the lens from automatically extending back to that position, resulting in an error that cannot be cleared by the owner..."

The risks? No doubt some user missed taking the one picture that would have won them a Pulitzer. Mere aggravation for all other users affected. Nikon is out a bunch of \$\$'s (or yen) involved in the cycle of recall, debug, reprogram a bunch of cameras.

Craig Mautner, Wind River Services, 10505 Sorrento Valley Road #1,  
San Diego, CA 92121-1608 1-858-824-3065 craig.mautner@windriver.com

---

## **Secure in, insecure out**

Jeremy Epstein <jepstein@acm.org>

Wed, 26 Dec 2001 09:27:48 -0500

As readers of RISKS know, many Internet users think that HTTPS is equivalent

to security. Here's an example where that went badly wrong.

My employer uses an online service to handle signups for the flexible spending plan (\*). It uses an HTTPS form to collect the usual personal info: name, address, social security number, and amount to be deducted. So far, so good. I don't know what it does with the information (presumably puts it in a database, which has it's own issues). Then they e-mail the information back to the user for confirmation, including the SSN.

Interestingly, \*someone\* at the company understood the risks, because their "security and privacy" policy on their home page notes that unencrypted e-mail is not safe. (\*\*) Whoever wrote that policy obviously wasn't working with the people building the system.

The response when we pointed the problem out was "we use HTTPS, so we're secure". After several rounds of back-and-forth with the vendor, they admitted the problem, and proposed to fix it early next year. Since this is software that gets used once a year (to meet the Dec 31st deadline), that was clearly a silly proposal, since all users would be forced into using the incorrect version. So after some arm-twisting, they changed the confirmation message to eliminate all but the last 4 digits of the SSN. A big improvement.

The risk here is that this is a commercial system that's presumably used by many other companies besides ours. How many other companies use this flawed system and never objected? And how many other equivalent systems are there

out on the net? If I were looking for an easy way to commit identity theft, I'd be monitoring e-mails coming out of that company... chances are there's a lot of good info! (Which is why I'm not giving their name or URL!)

-----

(\*) A flexible spending plan is established by US tax law to allow tax-free deductions from salary into an account which can then be used to pay for medical or child care expenses. By law, you have to decide by December 31st how much money will be deducted in the following year, and you (generally) can't change that decision once it's made. Also, any unspent money is not returned to the employee, so it's important to estimate accurately. Because of the legal Dec 31st deadline, it wasn't possible/feasible to wait for a more appropriate resolution of the problem.

(\*\*) I did a Google search on the actual phrase used on their Web page to see if it would disclose who the vendor is. They were the only vendor of their type who used the particular phrase, which is why I haven't quoted it verbatim, but it seems to be a catch phrase used in MANY security and privacy policies. So perhaps they just cut & pasted it without having a clue what it meant.

--Jeremy

P.S. Yes, I understand there are a lot of other risks in this system besides just sending the SSN unencrypted. This was just particularly egregious.

## **✶ Assume no safety ...**

Peter Houppermans <Peter.Houppermans@paconsulting.com>

*Mon, 17 Dec 2001 16:43:01 -0000*

I came across an ad in *\*Computing\** for the new Samsung GT9000Pro notebook,  
one of the laptops following the trend to have a fingerprint scanner built  
in. Envisage: switch on the machine, press thumb and you're logged in (for  
the sake of Administrators thumbs, I hope they allow a file update for a  
mass rollout, but I digress ;-).

Now, after this highly sophisticated, technically advanced piece of  
biometric technology has reliably authenticated, you can immediately start  
to work on your Corporate network ..

.. via its built-in Wireless LAN network card.

Duh.

The RISK: assuming that a fancy front-end (the scanner) implies a completely  
secure system.

Peter Houppermans, PA Consulting Group Ltd

---

## **✶ Re: Identity theft without prior knowledge of SSN**

Brett Harmond <brett\_harmond@yahoo.com>

*Mon, 17 Dec 2001 09:20:32 -0800 (PST)*

A few years ago I had the pleasure of writing a program to pull credit reports electronically. During my testing, I learned that one only needs two of the following three pieces of information: Name (defined by last name and only the first three characters of the first name), SSN, and Address. Given any two of the three and making up the third, you can obtain a legitimate credit report. Considering how easy it is to find anyone's name and address, this makes it a piece of cake to get their social security number and other interesting information.

---

## ⚡ Mersenne prime exponent wrong ([RISKS-21.82](#))

<KCKnowlton@aol.com>

*Sun, 16 Dec 2001 20:26:19 EST*

(On the RISK of manually inputting digits:)

That new Mersenne prime as given on the cited Web page is  
 $2^{(13,466,917)} - 1$ , not  $2^{(12,466,917)} - 1$ .

Shall we call this another off-by-one error, or off-by-two-to-the-millionth? Ken Knowlton

---

## ⚡ Re: Computer will drive 820 passengers at 68 mph (Norton, [R 21-82](#))

<Ian.Entecott@tas.alcatel.ca>

*Mon, 17 Dec 2001 08:29:01 -0500*

The train control system being installed at JFK Airport is a SELTRAC system made by the Transport Automation division of Alcatel Canada Inc. Alcatel have installed several such systems around the world including the Docklands Light Railway, London, UK; the SkyTrain, Vancouver, BC, Canada and the LRT2, Kuala Lumpur, Malaysia. All operate to similar specifications given in Daniel Norton's posting; the DLR carries 130,000 passengers a day using 30 single and double vehicle driverless trains and has been in operation since 1993 without an accident to passengers or staff. Regular readers of RISKS will already be saying to themselves that operating software problem free for several years is no guarantee that there are no problems waiting to be revealed but I hope Alcatel's record in developing automatic train control systems will reassure Daniel that the AirTrain will provide safe, reliable transport for the passengers and staff of JFK Airport.

Ian Entecott, Alcatel Canada Inc., Transport Automation Systems, 1235 Ormont Drive, Weston, Ontario, L3X 1N2, Canada.

---

**✶ Re: Computer will drive 820 passengers at 68 mph ([R-21.82](#))**

Jonathan Thornburg <jthorn@aei.mpg.de>  
*Sun, 16 Dec 2001 15:37:10 +0100*

Vancouver, Canada's "Skytrain" light rail transit system has been operational since 1986, and currently carries an average of 110,000

people per day at cruising speeds of 72 km/hr, with a fleet of 150 cars on 29 km of track, (A major extension is currently under construction.) The system is fully computer-controlled: there are \*no\* drivers or (apart from roving fare checkers and security guards) any other transit personnel in the cars. Indeed, there are no driver's cabs in the cars. Further details at [http://city.vancouver.bc.ca/commsvcs/planning/atoz/A\\_ALRT.htm](http://city.vancouver.bc.ca/commsvcs/planning/atoz/A_ALRT.htm) <http://www.questercorp.com/transit/index.html>

I lived in Vancouver during the system's initial commissioning and for some years thereafter, and I don't recall any serious problems being reported in the local press.

Jonathan Thornburg, Max-Planck-Institut fuer Gravitationsphysik (Albert Einstein Institut), Golm, Germany <http://www.aei.mpg.de/~jthorn/home.html>

---

## **✶ Re: Computer will drive 820 passengers at 68 mph**

Curt Sampson <cjs@cynic.net>  
*Mon, 17 Dec 2001 13:38:34 +0900 (JST)*

The biggest RISK here is lack of even basic research on the part of a worried person, I'd say. [... some duplication on Alcatel deleted. PGN]

As it turns out, for many of the safety systems, the technology is not even that new, or even computer-related. I asked a friend of mine who

worked on this Alcatel system for his comments. He said:

> Well, most automated systems use some kind of physical interlocking  
> system that guarantees safety. The trains are driven by computer, but  
> because of the nice tidy one dimensional network problem, it's fairly  
> easy to contain the safety critical portion into this interlocking.  
> In some systems it's actually completely mechanical, with the computer  
> (I kid you not) driving the motion of metal bars pneumatically. An  
> unsafe route cannot be set without one iron bar passing through  
> another iron bar.  
>  
> I guess the point is that this interlocking is present whether the  
> system is human controlled or computer controlled: the only real  
> difference is that in an automated system it's a computer paying  
> attention to the signals and there is a mechanism to halt the train if  
> a signal is ignored. In a human operated system an unsafe route still  
> can't be set because of the interlocking, but a human can skip a  
> signal and human systems usually don't include very effective  
> mechanisms for forcing a stop when a signal is blown.  
>  
> Short version: we have hundreds of years of experience building safety  
> critical train systems and in most cases these systems are still in  
> use to protect the train and passengers---even when a computer is  
> doing the driving.

(Actually, I've seen some pretty effective systems for making sure that human-driven trains stop. On the New York subways, there is a

lever on  
the tracks at each signal that pops up when the light is red. If  
the  
driver attempts to pass the signal when this lever is up, the  
lever will  
trigger a switch under the car that turns on the brakes. If you  
stand  
at the middle or the head end of a subway platform in NYC, you  
can see  
this system in operation.)

Getting out of the safety area, I suppose the RISKSs might  
include loss  
of service due to computer failures. But then again, given the  
level  
of train automation we're using even in systems with drivers,  
the risk  
appears not significantly different. (A severe computer failure  
in the  
train control systems on a system with drivers still brings the  
entire  
system to a halt; drivers rely on the signaling to make sure  
that they  
are taking safe actions.)

So to this reader at least, the risks are not at all obvious.  
We've had  
automated systems shuttling around groups of "820 people at 68  
mph" for a  
long, long time now, with an excellent safety record and,  
overall, a  
significant improvement in the number of people a system can  
move as  
compared to one with human drivers.

Curt Sampson <cjs@cynic.net> +81 90 7737 2974 <http://www.netbsd.org>

---

**✶ Re: Computer will drive 820 passengers at 68 mph (Norton, [R-21.82](#))**

"Jeff Jonas" <jeffj@panix.com>

Fri, 14 Dec 2001 22:57:29 -0500 (EST)

The Port Authority of NY & NJ already operates such train-systems:

\* The PATH system mostly crosses the Hudson river, linking NY to NJ (the link to lower Manhattan was at the World Trade Center, a temporary station might open in 2 years). It looks like a subway system: high tech signalling and communications but the train's still totally under the motorman's control.

\* The monorail around Newark airport seems fully or highly automated.

It was recently extended to the Northeast Corridor train lines (N.J. Transit and Amtrak trains)

[PS: I think the Port Authority of NY/NJ also owned/operated the World Trade Center. Related to this: after the first bombing, the twin towers were criticized for not meeting New York City fire codes since it was not accountable to NYC being a Port Authority project! Also related: before 9/11, there were efforts to "privatize" the New York City airports but now with the move towards federal oversight, the Port Authority might keep control]

\* The Delaware River Port Authority of Pennsylvania and New Jersey operates PATCO: a tiny train system similar to PATH: see <http://www.drpa.org/patco/>

I remember the PATCO Hi-Speedline has an operator sitting in a little platform with a curtain, more like a bus-driver than the usual booth for a train engineer. Under normal operation, the train runs hands

free, the operator just opens and closes the doors. The operator seems to take full control of the train when running on the alternate tracks.

In Miami Florida, there's some elevated people-mover that's fully automated, no operators on the little trolley-like monorail-like system. But it moves slowly. See:

<http://www.co.miami-dade.fl.us/transit/>

Miami-Dade Transit

<http://www.fta.dot.gov/library/technology/apm/apmrev.html>

AUTOMATED PEOPLE MOVER APPLICATIONS: A WORLDWIDE REVIEW

<http://faculty.washington.edu/~jbs/itrans/detroit.htm>

Detroit Downtown Peoplemover

<http://faculty.washington.edu/~jbs/itrans/miami.htm>

Miami Metromover - The First Automated Downtown Peoplemover in the U.S.

[The shuttle between Grand Central and Times Square in New York City was

fully automated MANY years ago. PGN]

---

## **Re: Computer will drive 820 passengers at 68 mph**

Jacob Sparre Andersen <sparre@nbi.dk>

*Sun, 16 Dec 2001 17:24:56 +0100*

The Paris metro line 14 is fully automated, and does not seem to have any special problems. The automated train control system for line 14 was implemented in Ada (a programming language designed with the goal of getting

reliable software), and the implementation was tested using a theorem proof system.

The future Copenhagen airport metro is supposed to be fully automated, but nobody knows if it is going to work or not (yet).

I definitely prefer the Paris metro line 14 to the roads of Copenhagen and Paris.

Jacob

---

**✶ Re: Computer will drive 820 passengers at 68 mph (Norton, [R-21.82](#))**

"Anthony W. Youngman" <Anthony.Youngman@ECA-International.com>  
*Mon, 17 Dec 2001 13:24:58 -0000*

Well, there's always the Docklands Light Railway (DLR) in London which works fine and, as far as I know, has never had an accident. [SEE PGN NOTE BELOW.] And the engineers comment that there is \*less\* likelihood of an accident with an automated system, which sounds right given the fact that we've had several very nasty accidents due to drivers ignoring signals recently.

Mind you, that "drivers ignoring signals" is another example of RISKY behaviour. The sequence of signals from danger to safe is "red", "single yellow", "double yellow", "green". Given that due to crowding most trains go

through most signals on double yellow, all too often they go through a single yellow without realising it (the in-cab warning is IDENTICAL for both). So a train going at near full speed suddenly realises the signal in front is red, having missed the single yellow "slow down" warning, and is at serious risk of overrunning the red because it can't stop in time (or even worse, misses the red completely, and then cancels the cab warning because, again, IT IS THE SAME IN-CAB SIGNAL!).

[In [RISKS-5.29](#), Mark Brader notes a Docklands crash on 10 Mar 1987, at the Island Gardens station. The train crashed through the station buffers and hung off the end of the elevated track. Required modifications that would have prevented the accident had not yet been installed. PGN]

---

## ⚡ Re: Computer will drive 820 passengers at 68 mph

Andrew Roberts <andrew.roberts@automationpartnership.com>  
*Mon, 17 Dec 2001 12:39:59 +0100*

This sounds very similar to the system at STN London Stanstead. There, the main terminal is separate from satellites where the gates are located. A fully automated, driverless guided busway runs between these, going underground to reach the satellites. I say busway because the vehicles have rubber tyres rather than running on rails.

Carriages (originally 1, but now 2 coupled together, I think

there's room  
for 3 at the stations) travel at up to 40mph (my estimate), and  
carry  
similar number of passengers as the JFK system.

This has been in operation since the early nineties, without a  
single  
breakdown when I've been on it (unlike the rest of the UK  
railway system).

Andrew Roberts, The Automation Partnership(Cambridge) Ltd, York  
Way,  
Royston, Herts, SG8 5WY, UK <http://www.automationpartnership.com>

---

## **⚡ Re: Computer will drives 820 passengers at 68 mph (Norton, [R-21.82](#))**

<Jens.Braband@web.de>

Wed, 19 Dec 2001 20:40:41 +0100

While the risk of automatic guided transport is obvious, it is  
nothing new.

Automatic systems have been in operation since the early 80's  
mainly in  
metros and airport shuttles. For example, the Web site of the  
market  
leader, Matra Transport (<http://www.matra-transport.fr/>) shows  
this clearly  
with systems being realised all over the world. It must also be  
acknowledged that the automatic guided transport systems seem to  
have a  
clean safety record so far and that also high-speed trains,  
although not  
being fully automated, have to rely to a great extent on  
computer guidance.

[Matra is also responsible for the Ariane 5 and Taipei subway  
system

(which suffered a computer crash, but no accidents, on 3 Jun 1986).

See [RISKS-18.17](#) and 18.19. PGN]

---

## **✶ Re: Computer will drive 820 passengers at 68 mph (Norton, [R-21.82](#))**

Jerrold Leichter <jerrold.leichter@smarts.com>

*Sun, 23 Dec 2001 17:55:14 -0500 (EST)*

Such systems are common, and have been common for many years. The commonality may not be obvious because of a difference in physical orientation: The ones in wide use have tracks running vertically. We call them elevators. Granted, elevators don't attain the same rate of speed - about 15 mph seems to be the limit - but a falling car could easily exceed it. And granted few if any elevator cars carry 820 passengers - but there are certainly many large buildings whose entire elevator system, during peak periods, carries much greater passenger loads.

Ah, but elevators just go up and down a single isolated shaft. Actually, first of all that's not true in modern buildings; second, the JFK rail system appears to follow pretty much the same model. (This is based on personal observation of the system as it's being built. It will run on a pair of tracks built over a highway, completely isolated from all other traffic.)

A large, complex system of trains on various interconnected tracks poses difficult problems which we probably aren't ready to deal with fully automated controls. A simple back-and-forth system with no external connections and a limited number of trains is quite a different story.

Will this system be hazard- and problem-free? Only time will tell - but there's no reason I can see to believe that it would be safer so if a human being - whose ability to respond quickly and accurately after months of numbing routine going back and forth between the same 5 or 6 stations would surely be severely taxed - were standing at the controls. Actually, as many years of experience has shown, a human being - unaided - would do very badly at this kind of job. That's why railroad systems have various safety automated safety devices. For that matter, so do elevators - and they introduced them when "elevator operator" was still a job description. If there's reason to believe that the JFK system has scrimped on such systems, that's another issue - but my reaction would be no different from hearing that a new digitally-controlled elevator had eliminated the mechanical emergency brakes that have been standard for the better part of a century.



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 21: Issue 84**

**Saturday 5 January 2002**

## Contents

- [Peak time for Eurorisks](#)  
[Paul van Keep](#)
- [More Euro blues](#)  
[Paul van Keep](#)
- [ING bank debits wrong sum from accounts](#)  
[Paul van Keep](#)
- [Euro bank notes to embed RFID chips by 2005](#)  
[Ben Rosengart](#)
- [TruTime's Happy New Year, 2022?](#)  
[William Colburn](#)
- [Airplane takes off without pilot](#)  
[Steve Klein](#)
- [Harvard admissions e-mail bounced by AOL's spam filters](#)  
[Daniel P.B. Smith](#)
- [Risk of rejecting change](#)  
[Edward Reid](#)
- [Security problems in Microsoft and Oracle software](#)  
[NewsScan](#)
- ["Buffer Overflow" security problems](#)  
[Henry Baker](#)

[PGN](#)

● [Sometimes high-tech isn't better...](#)

[Laura S. Tinnel](#)

● [When a "secure site" isn't](#)

[Jeffrey Mogul](#)

● [Info on RISKS \(comp.risks\)](#)

---

## ✶ Peak time for Eurorisks

Paul van Keep <paul@sumatra.nl>

*Fri, 28 Dec 2001 14:38:29 +0100*

There was a veritable plethora of Euro related gaffes just before the final changeover. A short overview of what has happened:

\* A housing society in Eindhoven (The Netherlands) has sent out bills for next month's rent in Euro's. But the amount on it is the same as last month's rent, which was in guilders, a 2.2x increase. The society has declared that anyone who paid the incorrect amount will be fully refunded and will get a corrected bill later.

\* A branch of ING bank in Blerick inadvertently inserted the wrong cassette into an ATM, which began to give out Euro bills instead of Guilders. This was illegal before January 1st, 2002. The bank has traced the bills and all but 10 euro have already been returned.

\* Rabobank has made an error in it's daily processing of 300,000 automatic transfers. Instead of transferring guilders, the transfers were made in

Euro's, again 2.2x what should have been transferred. The bank hopes to have corrected the mistake before 6pm tonight (Due to the Euro changeover, no banking activity will take place in any of the Euro countries on monday).

\* (Just somewhat related:) Two companies thought they were being really smart by putting Eurobills in Christmas gifts for their employees. They have been ordered by the Dutch central bank to recover all those bills or face charges.

---

## **⚡ More Euro blues**

Paul van Keep <paul@sumatra.nl>

*Thu, 3 Jan 2002 22:44:37 +0100*

The Euro troubles keep coming in. Even though banks have had four to five years to prepare for the introduction of the Euro, things still go wrong. Yesterday and today over 200 smaller Dutch post offices have had to remain closed because of computer problems relating to the Euro changeover. It is still unclear whether the situation will finally be resolved tomorrow.

---

## **⚡ ING bank debits wrong sum from accounts**

Paul van Keep <paul@sumatra.nl>

*Fri, 4 Jan 2002 09:45:07 +0100*

About 51,000 customers who withdrew money from their ING Bank account on 1 & 2 Jan 2002 (through an ATM) have had the wrong amount debited from their account. The bank hasn't yet given an explanation for the error other than to suspect that it was related to the high stress their systems were under during the first few days of the new year. The amounts debited from customer accounts was a hundred times what they withdrew from the ATMs. This got some people into trouble when their balance went negative and they could no longer use their bank PIN card to pay with in shops. ING Bank corrected the error yesterday.

On a related note, my wife withdrew Euros from an ATM yesterday and the printed receipt came up blank. My guess is that the ink ribbon on the embedded matrix printer ran out. Bank personnel are working like crazy to feed the machines with Euro bills and simply forget to check the printer. If her bank makes a mistake similar to the one ING made, she would have a hard time proving that she didn't withdraw 10000 Euro.

---

## **✶ Euro bank notes to embed RFID chips by 2005**

Ben Rosengart <ben@narcissus.net>  
*Thu, 27 Dec 2001 15:27:20 -0500*

The European Central Bank is working with technology partners on a hush-hush

project to embed radio frequency identification tags into the very fibers of euro bank notes by 2005. Intended to foil counterfeiters, the project is developing as Europe prepares for a massive changeover to the euro, and would create an instant mass market for RFID chips, which have long sought profitable application. <http://www.eetimes.com/story/OEG20011219S0016>

I hardly know where to begin even thinking about the RISKS involved.

[Those who are Europeein' may need a Eurologist to detect bogus chips. PGN]

---

## ⚡ TruTime's Happy New Year, 2022?

"Schlake (William Colburn)" <schlake@nmt.edu>  
*Wed, 2 Jan 2002 12:22:14 -0700*

Apparently (from the postings on comp.protocols.time.ntp) some TruTime GPS units suddenly jumped 1024 weeks into future sometime around New Year's Day 2002.

[GPS units have jumped 1024 weeks into the past before (R-18.24, R-20.07).  
Back to the future is a nice twist. PGN]

---

## ⚡ Airplane takes off without pilot

Steve Klein <gpmguy@pwb.com>

*Fri, 28 Dec 2001 09:01:56 -0500*

An empty plane took off by itself and flew 20 miles before crashing in California's rural Napa County. The two-seater Aeronica Champion had a starter system requiring the pilot to get out and hand-crank the engine.

[\*Wall Street Journal\*, 28 Dec 2001]

---

## **⚡ Harvard admissions e-mail bounced by AOL's spam filters**

"Daniel P.B. Smith" <dpbsmith@bellatlantic.net>

*Tue, 01 Jan 2002 06:42:26 -0500*

According to today's Globe, AOL's spam filters rejected e-mail sent by Harvard's admissions department to anxious applicants. The interesting thing is that "AOL officials could not explain" why their servers identified these e-mail messages as spam. No explanation, no responsibility, apparently no indication of anything that Harvard could do to avoid the problem in the future. Just one of those things, like the weather.

Despite jokes, USPS "snail mail" is very highly reliable. Those of us who have used e-mail for years are aware that it is much less reliable; for example, Verizon DSL's mail server slowed to a crawl for several months last year, and during that time period less than half of e-mail I sent from another account to test it were actually received. Antispam

filters  
decrease this reliability further.

The facile name "e-mail" was helpful in the eighties as a characterization of a form of electronic communication. However, there is a risk that the name may mislead people into assuming that it is comparable in reliability to postal mail.

Let us hope that organizations do not begin use e-mail for communications more important than university admissions letters, in the name of "security" (and cost reduction).

[The AOL Harvard problem was noted by quite a few RISKS readers. TNX]

---

## ✂ Risk of rejecting change (Re: Sampson, [RISKS-21.83](#))

Edward Reid <edward@paleo.org>  
*Fri, 28 Dec 2001 10:26:42 -0500*

> Mind you, that "drivers ignoring signals" is another example of RISKy  
> behaviour.

Perhaps we need a parallel forum: FORUM ON RISKS TO THE PUBLIC FROM THE USE OF HUMANS IN TECHNOLOGY. While research on human safety factors is widespread, comments in this forum often treat human-based systems as the baseline and assume that automation can only create risks. Comments often fail to consider improvements in safety from automation,

much

less more widely ramified benefits such as improved health resulting from our ability to transfer resources to health care.

What would happen in a forum devoted to asking the opposite question?

That is, "what are the risks or benefits of introducing human actors into a given system?".

At least, considering the question can provide some needed balance.

It's a way of considering the RISK of rejecting change.

Edward Reid

[Not ANOTHER forum! From the very beginning, RISKS has discussed risks

due to people as well as risks to people due to technology (which

typically are due to people anyway!). There's nothing new there. PGN]

---

## **Security problems in Microsoft and Oracle software**

"NewsScan" <newsscan@newsscan.com>

*Fri, 21 Dec 2001 08:47:58 -0700*

Two top companies have issued new statements acknowledging security flaws in

their products: Microsoft (Windows XP) and Oracle (the 9i application

server, which the company had insisted was "unbreakable."

Resulting from a

vulnerability called "buffer overflow," both problems could have allowed

network vandals to take over a user's computer from a remote location.

Microsoft and Oracle have released software patches to close the security holes, and a Microsoft executive says: "Although we've made significant strides in the quality of the software, the software is still being written by people and it's imperfect. There are mistakes. This is a mistake." (San Jose Mercury News 21 Dec 2001; NewsScan Daily, 21 December 2001) <http://www.siliconvalley.com/docs/news/svfront/secur122101.htm>

---

## ✶ "Buffer Overflow" security problems

Henry Baker <hbaker1@pipeline.com>

*Wed, 26 Dec 2001 21:19:22 -0800*

I'm no fan of lawyers or litigation, but it's high time that someone defined "buffer overflow" as being equal to "gross criminal negligence".

Unlike many other software problems, this problem has had a known cure since at least PL/I in the 1960's, where it was called an "array bounds exception". In my early programming days, I spent quite a number of unpaid overtime nights debugging "array bounds exceptions" from "core dumps" to avoid the even worse problems which would result from not checking the array bounds.

I then spent several years of my life inventing "real-time garbage collection", so that no software -- including embedded systems software -- would ever again have to be without such basic software error checks.

During the subsequent 25 years I have seen the incredible havoc wreaked upon the world by "buffer overflows" and their cousins, and continue to be amazed by the complete idiots who run the world's largest software organizations, and who hire the bulk of the computer science Ph.D.'s. These people know better, but they don't care!

I asked the CEO of a high-tech company whose products are used by a large fraction of you about this issue and why no one was willing to spend any money or effort to fix these problems, and his response was that "the records of our customer service department show very few complaints about software crashes due to buffer overflows and the like". Of course not, you idiot! The software developers turned off all the checks so they wouldn't be bugged by the customer service department!

The C language (invented by Bell Labs -- the people who were supposed to be building products with five 9's of reliability -- 99.999%) then taught two entire generations of programmers to ignore buffer overflows, and nearly every other exceptional condition, as well. A famous paper in the Communications of the ACM found that nearly every Unix command (all written in C) could be made to fail (sometimes in spectacular ways) if given random characters ("line noise") as input. And this after Unix became the de facto standard for workstations and had been in extensive commercial use for at least 10 years. The lauded "Microsoft programming tests" of the 1980's were designed to weed out anyone who was careful enough to check for

buffer

overflows, because they obviously didn't understand and appreciate the intricacies of the C language.

I'm sorry to be politically incorrect, but for the ACM to then laud "C" and its inventors as a major advance in computer science has to rank right up there with Chamberlain's appeasement of Hitler.

If I remove a stop sign and someone is killed in a car accident at that intersection, I can be sued and perhaps go to jail for contributing to that accident. If I lock an exit door in a crowded theater or restaurant that subsequently burns, I face lawsuits and jail time. If I remove or disable the fire extinguishers in a public building, I again face lawsuits and jail time. If I remove the shrouding from a gear train or a belt in a factory, I (and my company) face huge OSHA fines and lawsuits. If I remove array bounds checks from my software, I will get a raise and additional stock options due to the improved "performance" and decreased number of calls from customer service. I will also be promoted, so I can then make sure that none of my reports will check array bounds, either.

The most basic safeguards found in "professional engineering" are cavalierly and routinely ignored in the software field. Software people would never drive to the office if building engineers and automotive engineers were as cavalier about buildings and autos as the software "engineer" is about his software.

I have been told that one of the reasons for the longevity of the Roman bridges is that their designers had to stand under them when they were first used. It may be time to put a similar discipline into the software field.

If buffer overflows are ever controlled, it won't be due to mere crashes, but due to their making systems vulnerable to hackers. Software crashes due to mere incompetence apparently don't raise any eyebrows, because no one wants to fault the incompetent programmer (and his incompetent boss). So we have to conjure up "bad guys" as "boogie men" in (hopefully) far-distant lands who "hack our systems", rather than noticing that in pointing one finger at the hacker, we still have three fingers pointed at ourselves.

I know that it is my fate to be killed in a (real) crash due to a buffer overflow software bug. I feel like some of the NASA engineers before the Challenger disaster. I'm tired of being right. Let's stop the madness and fix the problem -- it's far worse, and caused far more damage than any Y2K bug, and yet the solution is far easier.

Cassandra, aka Henry Baker <hbaker1@pipeline.com>

---

✶ **"Buffer Overflow" security problems (Re: Baker, [RISKS-21.84](#))**

Peter G Neumann <Neumann@CSL.sri.com>  
*Wed, 26 Dec 2001 21:19:22 -0800*

Henry, Please remember that an expressive programming language that prevents you from doing bad things would with very high probability be misused even by very good programmers and especially by programmers who eschew discipline; and use of a badly designed programming language can result in excellent programs if done wisely and carefully. Besides, buffer overflows are just one symptom. There are still lots of lessons to be learned from an historical examination of Fortran, Pascal, Euclid, Ada, PL/I, C, C++, Java, etc.

Perhaps in defense of Ken Thompson and Dennis Ritchie, C (and Unix, for that matter) was created not for masses of incompetent programmers, but for Ken and Dennis and a few immediate colleagues. That it is being used by so many people is not the fault of Ken and Dennis. So, as usual in RISKS cases, blame needs to be much more widely distributed than it first appears. And pursuing Henry's name the blame game, whom should we blame for Microsoft systems used unwisely in life- and mission-critical applications? OS developers? Application programmers? Programming language developers? Users? The U.S. Navy? Remember the unchecked divide-by-zero in an application that left the U.S.S. Yorktown missile cruiser dead in the water for 2.75 hours ([RISKS-19.88](#) to [94](#)). The shrinkwrap might disclaim liability for critical uses, but that does not stop fools from rushing in.

Nothing in the foregoing to the contrary notwithstanding, it would be very helpful if designers of modern programming languages, operating

systems, and application software would more judiciously observe the principles that we have known and loved lo these many years (and that some of us have even practiced!). Take a look at my most recent report, on principles and their potential misapplication, for DARPA's Composable High-Assurance Trustworthy Systems (CHATS) program, now on my Web site: <http://www.csl.sri.com/neumann/chats2.html>

---

## **✶ Sometimes high-tech isn't better**

"Laura S. Tinnel" <ltinnel@teknowledge.com>  
*Sat, 29 Dec 2001 17:19:30 -0500*

We're all aware that many companies have buried their heads in the sand on the security issues involved with moving to high-tech solutions in the name of convenience, among other things. When we're talking about on-line sales, educational applications, news media, and the like, the repercussions of such are usually not critical to human life, and therefore the trade-off is made. However, I've just encountered something that is, well, disconcerting at best.

Earlier today as I sat unattended in an examination room for a half hour waiting on the doctor to show up, I carefully studied the new computer systems they had installed in each patient room. Computers that access ALL patient records on a centralized server located elsewhere in the

building,  
all hooked up using a Windows 2000 domain on an ethernet based  
LAN.

Computers that contained accessible CD and floppy drives and  
that could be  
rebooted at the will of the patient. Computers hooked up to a  
hot LAN jack  
(oh for my trusty laptop instead of that Time magazine...) Big  
mistake #1 -  
the classic insider problem.

Once the doctor arrived and we got comfy, I started asking him  
about the  
computer system. (I just can't keep my big mouth shut.) Oh he  
was SO proud  
of their new fangled system. So I asked the obvious question -  
what would  
prevent me from accessing someone else's records while I sat  
here unattended  
for a half hour waiting for you to show up? With a big grin on  
his face, he  
said "Lots of people ask that question. We have security here;  
let me show  
you." Big mistake #2 - social engineering. Then he proceeded to  
show me that  
the system is locked until a password is entered. Of course, he  
said, if  
someone stole the password, then they could get in, but  
passwords are  
changed every 3 months. And, he continued, that's as secure as  
you can get  
unless you use retinal scans. (HUH?) I know all about this  
stuff, for you  
see "my dear", I have a masters degree in medical information  
technology,  
and I'm in charge of the computer systems at XXXX hospital. OK.  
Time to fess  
up. Doc, I do this for a living, and you've got a real problem  
here. 1, Have  
you thought about the fact that you have a machine physically in  
this room  
that anyone could reboot and install trojan software on? A: Well  
that's an

issue. 2. Have you thought about the fact that there's a live network connection in this room and anyone could plug in and have instant access to your network? A: You can really do that??? There's a guy that brings his laptop in here all the time. 3. I assume you are using NTFS (yes), have you locked down the file system and set the security policies properly? You do understand that it is wide open out of the box. A: I don't know what was done when the computers were set up. 4. Have you thought beyond just the patient privacy issue to the issue of unauthorized modification of patient records? What are you doing to prevent this? What could someone do if they modified someone else's records? Make them very ill? Possibly kill them? A: That's a big concern. (well, duh?) Then there was a big discussion about access to their prescription fax system that could allow people to illegally obtain medication. I didn't bother to ask whether or not they were in any way connected to the Internet. They either have that or modems to fax out the prescriptions. At least he said he'd talk to his vendor to see how they have addressed the other issues. Perhaps they have addressed some of these things and the doctor I was chatting with simply didn't know.

I'm not trying to come down on these doctors as I'm sure they have very good intentions. I personally think having the medical records on-line is a good idea in the long term as it can speed access to records and enable remote and collaborative diagnoses, potentially saving lives. But I'm not convinced that today we can properly secure these systems to protect the

lives they  
are intended to help save. (Other opinions are welcome.) And  
with the state  
of medical malpractice lawsuits and insurance, what could a  
breach in a  
computer system that affects patient health do to the medical  
industry if it  
becomes reliant on computer systems for storage/retrieval of all  
patient  
records?

A couple of things. First, I'm not up on the state of cyber  
security in  
medical applications. I was wondering if anyone out there is up  
on these  
things or if anyone else has seen stuff like this.

Second, if a breach in the computer system was made and someone  
was  
mistreated as a result, who could be held liable? The doctors  
for sure.

What about the vendor that sold and/or set up the system for  
them? Does "due  
diligence" enter in? If so, what is "due diligence" in cyber  
security for  
medical applications?

Third, does anyone know if the use of computers for these  
purposes in a  
physician's office changes the cost of malpractice insurance? Is  
this just  
too new and not yet addressed by the insurance industry? Is  
there any set of  
criteria for "certification" of the system for medical insurance  
purposes,  
possibly similar to that required by the FDIC for the banking  
industry? If  
so, is the criteria really of any value??

[This is reproduced here from an internal e-mail group, with  
Laura's  
permission. A subsequent response noted the relative  
benignness of past

incidents and the lack of vendor interest in good security -- grounds that we have been over many times here. However, Laura seemed hopeful that the possibility of unauthorized modification of patient data by anyone at all might stimulate some greater concerns. PGN]

---

## ✶ When a "secure site" isn't

Jeffrey Mogul <JeffMogul@acm.org>

*Fri, 28 Dec 2001 17:22:33 -0800*

Most security-aware Web users are familiar with the use of SSL to provide privacy (through encryption) and authentication (through a system of signatures and certificate authorities). We have also learned to check for the use of SSL, when doing sensitive operations such as sending a credit card number, by looking for the "locked-lock icon" in the lower margin of the browser window. (Netscape and Mozilla display an "unlocked lock" icon for non-SSL connections; IE appears to display a lock icon only for SSL connections.) Notwithstanding the risks (cf. Jeremy Epstein in [RISKS 21.83](#)) of assuming that the use of SSL means "totally secure," its use is at least a prerequisite for secure Web commerce.

A few months ago, I was using the Web site of an established catalog merchant (predating the Internet) to order merchandise with my credit card. This merchant (whose name I have changed to "MostlyInnocent.

com") displays a "VeriSign Secure Site - Click to verify" logo on almost every page, and I had no reason to distrust their security. I had just typed the card number into their order form when I realized that the browser's icon was in the unlocked state -- fortunately, before I submitted the page.

Aha! an allegedly "Secure Site" that wasn't using SSL. Something was fishy.

I verified that my credit card would have been sent in cleartext by running

"tcpdump", entering a made-up credit card number, and finding that number in the tcpdump trace.

At this point, I did click on the "VeriSign Secure Site - Click to verify" logo, which popped up a window proving the validity of the site's SSL authentication. This window did indeed use SSL (evidenced by the locked icon). Moreover, the merchant's "Privacy Policy" page says "sensitive information [...] is protected both online and off-line by state-of-the-art, industry-standard technology [...] what we believe to be the best encryption software in the industry - SSL."

I immediately complained to the site's maintainers (this was made somewhat trickier because the phrase "If you have any questions about the security at the Site, you can send an e-mail to:" wasn't followed by an e-mail address!). Their first response was

I checked with our Web master and was assured that our new site is secure.

Located on the right-hand side of our home page is the VeriSign logo, and

a customer can verify that our site is indeed "valid" and secure.

I replied, pointing out the bug in this statement. Within 3 hours, they responded again that they had fixed the problem, and I was able to successfully place an order using SSL. I suspect that MostlyInnocent.com had simply forgotten to use "https" instead of "http" in a URL somewhere in the order-entry path, which shows evidence of negligence, but nothing worse. (I have no idea how long their site was afflicted by this bug.)

However, the larger problem remains: the site design (and, at first, the site maintainers) relies heavily on the implication that the "Secure Site" logo proves the security of the site. Clearly, it does not prove very much.

True network security is an end-to-end property. Saltzer et al., in "End-to-end arguments in system design," relate that this has been known since at least 1973 (see Dennis K. Branstad. Security aspects of computer networks. AIAA Paper No. 73-427, AIAA Computer Network Systems Conf, Huntsville, AL, April, 1973). The best place to verify that a site is using SSL properly is therefore in the browser software. Modern browsers do a fairly good job of alerting the user to the use of SSL (via the locked icon) and to questionable SSL certificates (through various popups).

This implies that we should continue educating users to check for the locked icon when sending sensitive information (and, to be fair, the Privacy page at MostlyInnocent.com does say "While on a secure page, such as

our order form, the lock icon on the bottom of Web browsers [...] becomes locked.")  
The use of the "VeriSign Secure Site" logo actively subverts this training, because it is much more prominent on the screen, yet proves very little about the site's security.

I complained to VeriSign about this problem. After a terse (and somewhat irrelevant) response, they have not replied to several repeated e-mail messages. My guess is that VeriSign profits from the proliferation of this logo (by charging merchants for its use), and therefore has little interest in promoting the end-to-end (locked-icon) model.

I don't see any efficient way for VeriSign to verify that sites using the logo are properly using SSL. Perhaps they could audit these sites on a regular basis, but that would require significant investments (in software, client systems for running audits, and network bandwidth) and it still would not be as reliable as the end-to-end model.

Browser implementors might be able to provide some protection, on the other hand, by flagging the user's attempt to enter what appears to be a credit-card number on a non-SSL connection. (My browser could store a one-way hash function of all of my credit-card numbers, thus facilitating this check without risking the security of my numbers.) I'm not sure whether most browser vendors have any incentive to do that; most have much deeper security problems to solve.



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 21: Issue 85**

**Monday 7 January 2002**

## Contents

- [Yokoh Satellite loses control](#)  
[Paul Saffo](#)
- [More medical risks](#)  
[Clay Jackson](#)
- [Bogus dates for McAfee virus alerts](#)  
[William Colburn](#)
- [Re: Harvard admissions e-mail bounced by AOL's spam filters](#)  
[Simon Waters](#)  
[Danny Burstein](#)  
[Gordon Zaft](#)
- [Re: "Buffer Overflow" security problems](#)  
[Nicholas C. Weaver](#)  
[Dan Franklin](#)  
[Kent Borg](#)  
[Jerrold Leichter](#)  
[Henry Baker](#)
- [Re: Software glitch grounds new Nikon camera](#)  
[Dave Gillett](#)
- [REVIEW: "Incident Response", Kenneth R. van Wyk/Richard Forna](#)  
[Rob Slade](#)
- [Info on RISKS \(comp.risks\)](#)

## 🚨 Yokoh Satellite loses control

Paul Saffo <psaffo@iftf.org>

Sat, 05 Jan 2002 07:08:39 -0800

An unharmonic convergence of solar eclipse and satellite's "invisible orbit"...

SKY & TELESCOPE'S NEWS BULLETIN - JANUARY 4, 2002

For images and Web links for these items, visit <<http://www.skypub.com>>

### YOHKOH LOSES CONTROL

On December 14, 2001, the Japanese solar observatory Yohkoh began spinning out of control. Since then, all scientific operations have stopped, and it remains unclear when the craft will be operational again.

The problem began during last month's annular eclipse of the Sun. Yohkoh uses a Sun-centering system to determine its position at any given time. During the eclipse, the craft lost contact with the Sun, put itself into a "safe mode," and slowly began to drift off track and rotate. Normally this wouldn't have been a problem -- during its decade in orbit, Yohkoh has seen its share of eclipses. However, this event occurred during a rare period of the craft's orbit (known as an invisible orbit) when the craft was out of communication with Earth. Thus controllers on the ground couldn't detect (or compensate for) the craft's sudden roll.

Problems only got worse from there. Because of its slow roll, Yohkoh's solar panels no longer received direct sunlight. By the time ground controllers at the Kagoshima Space Center regained contact with the observatory, its batteries were very low and the craft had lost attitude control.

To fix the problem, scientists first established contact and turned off all the craft's science instruments in order to conserve power. Currently the craft is rotating slowly, about one rotation per minute. According to Loren Acton (Montana State University), head scientist of Yohkoh's solar X-ray telescope, in the spacecraft's current state, its solar panels only receive sunlight in spurts. "During flashes of illumination, electricity is produced," says Acton. Thus the first step toward recovery is for scientists to wait until the craft can charge up.

It's currently unclear when, and even if, scientists will regain control of the craft. But astronomers are hopeful. "It will take clever work to stop the roll and re-acquire the Sun," says Acton.

---

## **✶ More medical risks**

"Clay Jackson" <clayj@nwlinc.com>  
*Sat, 5 Jan 2002 19:13:40 -0800*

In [RISKS-21.84](#), "Laura S. Tinnel" <ltinnel@teknowledge.com> wrote about

risks of unattended, unlocked computers in patient and examination rooms.

Reminds me of a time a few years back when I visited my local HMO (they have their own facilities), and discovered a username, password and IP address on a PERMANENT sticker the side of a system (the monitor, actually) being used for Patient Registration. Needless to say, the first thing I did when I got home was 'ping' that address from my PC. Of course, it responded. When I tried 'telnet', it came back with 'Login:'. I didn't have the heart to try the credentials I'd seen. The NEXT thing I did was drop an e-mail to a friend who worked in IS at the HMO. I returned to the clinic two weeks later, and the sticker had been pasted over. I don't know if they've yet secured their network (we've since switched providers).

Clay Jackson <clayj@nwlinc.com>

---

## **✶ Bogus dates for McAfee virus alerts**

"Schlake ( William Colburn )" <schlake@nmt.edu>

*Fri, 4 Jan 2002 11:48:23 -0700*

<http://www.mcafeeb2b.com/avert/virus-alerts/default.asp>

When I go to McAfee virus alerts Web page I read the somewhat disconcerting line "This page current as of" (and it ends, without even a period). What am I to assume about the currentness of the page?

Turning on javascript gives me a slightly different answer that reads "This page current as of Monday, January 4th, 1971." So now I know that as of early January 1971 there are NO virus alerts for any 1980's era DOS boxes and 1990's/2000's era Windows boxes. That sure makes me feel a whole lot better. Not only are there no virus alerts, but the machines those alerts would be for haven't even been invented yet!

Oh wait, the clock on my machine is just wrong, and the Web page merely printed out the local concept of the day and year.

How much can I trust the page now? The concept of "current" is local to me, the reader, via javascript. I don't need to go out onto the Internet to download a current copy of the page from the McAfee Web site to get an "up to date" version, I just have to reload my locally cached copy and presto it has today's date on it, and I will never again have to worry about viruses alerts because there won't be any.

The risk here is that someone could look at this Web page and see an invalid date because either their machine has the wrong time or because the Web page was cached somewhere and not re-downloaded. The result would be that someone might not find out about an important (high risk) virus that could potentially do a lot of damage.

PS: I complained about this to McAfee using their online form about a month ago, and never heard anything back.

## **✉ Re: Harvard admissions e-mail bounced by AOL's spam filters ([R-21.84](#))**

Simon Waters <Simon@wretched.demon.co.uk>

Sat, 05 Jan 2002 22:17:51 +0000

'"AOL officials could not explain" - why their servers identified these e-mail messages as spam.'

Funny, because I can explain this, and have in previous submissions to comp.risks, as it happens to many mailing lists.

AOL mail servers delete e-mails after accepting them if they think they are spam, without notifying the intended recipient or the sender. They do this when they receive bulk mailings, although the exact circumstances that trigger it remain known only to the AOL mail administrators.

Anybody having set up a large e-mail lists knows this, you have to get bulk mailing servers white-listed by AOL. Presumably Harvard didn't do this.

AOL doesn't publicise this information, but I've had the basics confirmed by a former employee of AOL.

The only way to ensure you get the e-mail from lists you subscribe to is not to use AOL for your e-mail.

Hopefully someone at Harvard will explain the business consequences of such idiotic behaviour to AOL, in the meantime just use an ISP who knows what

they are doing, not for nothing did they get the nickname "America Offline".

[Similar comments from Jenny Holmberg. PGN]

---

## **✶ Re: Harvard admissions e-mail bounced by AOL's spam filters** **[\(R-21.84\)](#)**

danny burstein <dannyb@panix.com>

*Sat, 5 Jan 2002 18:31:22 -0500 (EST)*

First, the stories claimed that these e-mails "bounced" back to Harvard.

However, in my own experience with AOL's spam filters, most of the time that mail is simply sent to /dev/null. So the sender generally does not even get any notice that their e-mail was undelivered. Since I haven't seen any actual direct quote from a Harvard spokesrep I doubt any sort of ack was sent back.

Also note that a "bounce" message would take this whole saga out of the "risks" venue (or at least move it to the margin). Once the sender is advised of the problem different steps can be taken. And in this sort of situation, an e-mail bounce ten minutes after sending is far preferable to a USPS similar bounceback which would take days or weeks.

The second point is that the stories, again, claim that Harvard was putting information about this up on their Web page. I've been checking every few hours since the reports first appeared. Nothing about this has

appeared on  
their main page nor on any obvious links.

---

## **✶ Re: Harvard admissions e-mail bounced by AOL's spam filters ([R-21.84](#))**

Gordon Zaft <zaft@newmonics.com>  
*Mon, 07 Jan 2002 13:13:36 -0700*

Daniel Smith notes, "Let us hope that organizations do not begin use e-mail for communications more important than university admissions letters, in the name of "security" (and cost reduction)."

Alas, it's too late for that. My alma mater, The University of Arizona(tm) (really!) now requires all students to have and use an e-mail account for official correspondence. While it's true that problems with university-hosted e-mail are not likely to cause a problem (or to be caught if they are), many students are likely to forward these accounts to other accounts where they might run into this problem. It's disturbing.

UA's e-mail policy is online at  
<http://www.registrar.arizona.edu/emailpolicy.htm> .

---

## **✶ Re: "Buffer Overflow" security problems (Baker, [RISKS-21.84](#))**

"Nicholas C. Weaver" <nweaver@CS.Berkeley.EDU>  
*Sat, 5 Jan 2002 13:15:52 -0800 (PST)*

I agree with Henry Baker's basic assessment that buffer overflows, especially in code which listens to the outside world (and therefore vulnerable to remote attacks) should be classed as legally negligent. However, it seems to be nigh-impossible to get programmers to write in more semantically solid languages.

There is another solution: software fault isolation [1]. If the C/C++ compilers included the sandboxing techniques as part of the compilation process, this would eliminate the most deleterious effects of stack and heap buffer overflows: the ability to run an attacker's arbitrary code, with a relatively minor hit in performance (under 10% in execution time).

An interesting question, and one for the lawyers to settle, is why haven't these techniques been widely deployed? The techniques were being commercialized by Colusa Software as part of their mobile code substrate [2] in the mid 1990s. In March 1996, Colusa software was purchased by Microsoft and it seems effectively digested, thereby eliminating another potential mobile-code competitor, something Microsoft seemed to fear at the time.

The interesting RISK, and one which is probably best left to the lawyers, is that as a result, for over half a decade, Microsoft has owned the patent rights and the developments required to eliminate two of their biggest security headaches: unchecked buffer overflows and Active-X's basic "compiled C/C++" nature, yet seems to have done nothing with

them.

What is the liability involved when a company owns the rights to a technology which could greatly increase safety, at an acceptable (sub 10%) performance penalty, but does nothing to use it in their own products? Especially when the result is serious, widespread security problems which could otherwise be prevented?

[1] "Efficient Software-Based Fault Isolation", Robert Wahbe, Steven Lucco, Thomas E. Anderson, Susan L. Graham, in \*ACM SIGOPS Operating Systems Review\*, volume 27, number 5, December 1993, pp 203--216,

[2] "Omniware: A universal substrate for mobile code"

Nicholas C. Weaver nweaver@cs.berkeley.edu

---

## **✶ Re: "Buffer Overflow" security problems (PGN, [RISKS-21.84](#))**

Dan Franklin <dan@dan-franklin.com>

*Sun, 6 Jan 2002 11:40:50 -0500*

> Perhaps in defense of Ken Thompson and Dennis Ritchie, C (and Unix, for that matter) was created not for masses of incompetent programmers, but for Ken and Dennis and a few immediate colleagues.

Which only serves to emphasize Henry's point. The code that those "few immediate colleagues" wrote also suffered from buffer overflow problems.

Not only did many ordinary commands written at Bell Labs fail

given long  
enough lines, but in one early version of UNIX, the (written in  
C) login  
command had a buffer overflow problem that permitted anyone to  
login by  
providing sufficiently long input.

In other words, C buffer overflows have caused security problems  
ever since  
the language was created; and even the earliest users of C have  
been caught  
by it. If software were really an engineering field, we would  
learn as  
engineers do to avoid tools and methods that persistently lead  
to serious  
problems.

Note that gcc, the very popular GNU C Compiler, has experimental  
extensions  
to support bounds checking; see <http://gcc.gnu.org/extensions.html>. Let us  
hope that one of these extensions makes its way out of the  
laboratory soon.  
If it became a standard gcc option, the current sorry situation  
might begin  
to improve.

---

**✶ Re: "Buffer Overflow" security problems (Baker, [RISKS-21.84](#))**

Kent Borg <kentborg@borg.org>  
*Mon, 7 Jan 2002 11:47:16 -0500*

A good start, but as we have heard before, be careful what you  
wish for.

First, take a quick look at our current patent office (full of  
experts who  
still approve the silliest software patents) to judge whether

our legal system (full of someone's peers) will be able to handle the concept "buffer overflow".

Second, even though most open source software is written in C, it is still easier to assemble a reasonably secure Internet server out of common open source software than it is from the dominant proprietary options. And open source software is getting better in this regard.

On its face, however, it seems your proposal would have the effect of outlawing open source software.

Rather, we might consider putting the liability on those who use the software -- for even good software can be misapplied -- encouraging users to choose well written products, and creating a market for well written products.

Put another way, consider this example: instead of banning the "book of spells" we might instead sanction the "sorcerer's apprentice" who plugs an unprotected computer into the Internet and so lets the broomsticks fly. I don't think you'll get the results you desire.

Sure, maybe let the user pass on some blame to negligent companies, but let's not have the blame \*start\* at the individual programmer's keyboard.

Or, put in Roman terms, have the various management (including those who commission it) stand under the new bridge, not the stone carvers.

-kb, the programmer Kent who admits he has a conflict of interest here.

---

**✶ Re: "Buffer Overflow" security problems (Baker, [RISKS-21.84](#))**

Jerrold Leichter <jerrold.leichter@smarts.com>

*Mon, 7 Jan 2002 12:00:29 -0500 (EST)*

Henry Baker complains about the continuing stream of problems due to buffer overflows, and blames the C language. PGN repeats a number of common defenses for C:

- It's perfectly possible to write bad, buggy code in the best languages;
- It's perfectly possible to write good code in the worst languages;
- It's wrong to blame Ken Thompson and Dennis Ritchie (who, BTW, Mr. Baker did not) because they never intended for C and Unix to be used the way they are today;
- Expanding on this, spreading the blame for the use of inappropriate Microsoft systems in life- and mission-critical applications to just about every one who's ever touched a computer.

I've been a C programmer for some 20 years, a C++ programmer for 6. I know well the advantages of the languages. But I'm really tired of the excuses.

No, Thompson and Ritchie are not to blame. Anyone who actually reads what they've written over the years - papers or code - will know that

they understand the tradeoffs and make them very carefully. I wish my code could be as good as theirs!

Unfortunately, I can't say the same about much of the C and C++ culture that grew up around their inventions over the years. A programming community develops its own standards and styles, its own notions of what is important and what isn't important. These standard, styles, and notions are extraordinarily influential. Some of the influence is transmitted through teaching; much is transmitted through the code the community shares. The most pernicious influences in the C/C++ community include:

- An emphasis on performance as the highest goal. For the most recent manifestation of this, you need only look to the C++ Standard Template Library (STL). It has many brilliant ideas in it, but among the stated goals, from the first experiments, was to produce code "as efficient as the best hand-tuned code". "As \*safe\*" or "as \*reliable\*" were simply not on the table. The STL has attained its stated goals.

Yes, there are debugging versions with things like bounds checking, but "everyone knows" that these are for testing; no real C++ programmer would think of shipping with them.

- A large body of code that provides bad examples. Why are there so many buffer overflows in C code? The C libraries are, to this day, full of routines that take a pointer to a buffer "that must be large enough to

contain the result". No explicit size is passed. I'm told that the guys at AT&T long ago removed `gets()`, a routine like that which reads input, from their own library. It persists in the outside world - an accident waiting to happen. Some routines have only very recently even appeared in alternative versions that have buffer length arguments - like `sprintf()` and its relatives. Until `snprintf()` became widespread (no more recently than the last 5 years), it was extremely difficult to write code that safely wrote arbitrary data to an in-memory buffer. (If you think it's easy, here's a quick question: How large must a buffer be to hold the result of formatting an IEEE double in `f` format with externally-specified precision? Hint: The answer is *\*much\** larger than the "about 16" that most people will initially guess.)

As part of a C++ system I work on, I have a vector-like data structure. The index operation using `[]` notation is range-checked. For special purposes, there's an `UnsafeAt()` index operation which is not. Compare this to the analogous data structure in the C++ library, where `[]` is *\*not\** range checked and `at()` is. When the choice is between `a[10]` and `a.at(10)`, which operation will the majority of programmers think they are supposed to use? Which data structure would you rather see taught to the programmers who will develop a system your life will depend on? (BTW, extensive profiling has yet to point to `[]`'s range checking as a bottleneck, with the possible exception of the implementation

of a hash

table, where `unsafeAt()` could be used in a provably-correct way.)

- A vicious circle between programmers and compiler developers. C and C++

programmers are taught to write code that uses pointers, not indices, to

walk through arrays. (The C++ STL actually builds its data structures on

the pointer style.) So why should C/C++ compiler developers put a lot of

effort into generating good code for index-based loops? C/C++ programmers

are taught not to expect the compiler to do much in the way of common

sub-expression elimination, code hoisting, and so on - the earliest C

compilers ran on small machines and couldn't afford to. Instead, C/C++

programmers are taught to do it themselves - and the C language allows

them to. So why should C/C++ compiler developers bother to put much

effort here?

Put this together and you can see that checking your array accesses for

out-of-range accesses can be a really bad idea: Your check code could run

every time around the loop, instead of being moved out to the beginning as

a FORTRAN programmer would expect. I'm sure there are some - perhaps many

- C/C++ compilers today that would provide such optimizations. Given the

generality of C and C++, it can be a challenge, but the techniques exist.

However, it's an ingrained belief of C/C++ programmers - and a well-founded one - that they can't *\*rely\** on the availability of such

optimizations. (A FORTRAN programmer can't point to a standard in his

reliance on such optimizations, but no one today would accept a FORTRAN compiler that didn't do them.)

I haven't even touched on the closely related issue of the dangers of manual memory management, and the continuing refusal of the C/C++ community to accept that most programs, and certainly most programmers, would be better off along every significant dimension with even a second-rate modern memory allocator and garbage collector -- especially in the multi-threaded code that's so common today.

Is it *possible* to write reliable, safe code in C or C++? Absolutely -- just as it's *possible* to drive cross-country safely in a 1962 Chevy. Does that mean the seat belts, break-away steering columns, disk brakes, air bags, and many other safety features we've added since then are unnecessary frills?

Programming languages matter, but even more to the point, programming *culture* matters. It's the latter, even more than the former, that's given us, and will continue to give us, so much dangerous code. Until something makes it much more expensive than it is now to ship bad code -- and I believe that Mr. Baker is right, and the only thing that will do it is a few big liability judgments - nothing is likely to change. Unfortunately, liability judgments will bring other changes to the programming world that may not be nearly so beneficial.

## ⚡ Re: "Buffer Overflow" security problems (Baker, [RISKS-21.84](#))

Henry Baker <hbaker1@pipeline.com>

Sun, 06 Jan 2002 09:08:42 -0800

Ari Ollikainen wrote [to HB]:

> And hardware with separate instruction and data space would not  
> necessarily solve the buffer overflow problem but at the very  
least would  
> avoid the inevitable compromise of reliability... and the  
possibility of  
> corrupting running code.

> There was a time when ANY flavor of unix was considered an  
oxymoronic  
> concept in regard to reliability and security.

> Ari Ollikainen, OLTECO, Networking Architecture and Technology,  
> P.O. BOX 20088, Stanford, CA 94309-0088 1-415 517 3519  
Ari@OLTECO.com

Good point re separate I & D spaces ("Harvard" architecture).

One of the reasons why people like network "appliances" (i.e., non-programmable devices, except for firmware) is that they think that they are secure from viruses. But if they have any capability of executing code out of data space, then they are just as vulnerable to "buffer overflow" attacks. In fact, because of their supposed invulnerability, they are probably more susceptible, because no one bothers to run virus checking software on them. Henry

---

## **⚡ Re: Software glitch grounds new Nikon camera (Mautner, [RISKS-21.83](#))**

Dave Gillett <dgillett@deepforest.org>

*Wed, 26 Dec 2001 16:14:32 -0800*

About 18 months ago, I managed to get my Kodak digital camera into a state where it would not properly complete the power-up cycle, nor power down. I was able to clear this state by removing the batteries; on re-insertion, a normal power-down state presented itself, and power-up proceeded normally.

The jammed condition was the result of timing of some user interactions while other actions were in progress; I have never been able to reproduce it.

---

## **⚡ REVIEW: "Incident Response", Kenneth R. van Wyk/Richard Forna**

Rob Slade <rslade@sprint.ca>

*Mon, 7 Jan 2002 10:01:47 -0800*

BKINCRES.RVW 20011001

"Incident Response", Kenneth R. van Wyk/Richard Forna, 2001, 0-59600-130-4, U\$34.95/C\$52.95

%A Kenneth R. van Wyk ken@incidentresponse.com

%A Richard Forna rick@incidentresponse.com

%C 103 Morris Street, Suite A, Sebastopol, CA 95472

%D 2001

%G 0-59600-130-4

%I O'Reilly & Associates, Inc.

%O U\$34.95/C\$52.95 800-998-9938 fax: 707-829-0104 nuts@ora.com  
%P 214 p.  
%T "Incident Response"

Incident response has, in the past, received short shrift in security literature. It is also a rather vague term: what type of an incident are we talking about? how big? What type of response are we considering? protective? defensive? offensive? The authors have provided us a starting point for consideration and the benefit of some years of experience, but this work is, unfortunately, less detailed than it might have been.

Chapter one does not do a good job of defining incident response: the examples are instructive, but the material wanders through a number of topics without developing any central focus. There is an examination of the strengths and shortcomings of various types of response teams, such as those internal to companies, related to vendors, or established by security management companies, in chapter two. Planning, in chapter three, has some good points to consider, but doesn't offer a lot of guidance. Chapter four, entitled "Mission and Capabilities," seems to be the core of the book, touching on staff, positions, training, legal considerations, procedures, and other issues. A wide-ranging list of attack types, albeit with very terse descriptions, is given in chapter five. The incident handling model presented in chapter six is vague but reasonable. Chapter seven contains quick overviews of a number of detection tools, mostly software. A few

resources, generally Web sites, are given in chapter eight.

This book is the result of considerable background and practice. While there are no obvious errors and the material presents good advice, it is hard to be excited about the result. Overall, the book seems to lack direction, and fails to present a structured and clear guide to the preparations necessary for dealing with computer incidents. However, in the absence of other material it is better than nothing, and does raise the issues to be addressed.

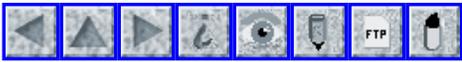
In response to the first draft of this review, one of the authors has responded that the intent of the book was not to address the techniques of incident response, but to provide management with an understanding of the subject. That statement fits with the text, but is in some opposition to the assertion in the preface that the book is aimed at all who would need to respond to incidents, including systems administrators and other technical people.

copyright Robert M. Slade, 2001    BKINCRES.RVW    20011001  
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 21: Issue 86**

**Thursday 10 January 2002**

## Contents

- [Credit-card cloners' \\$1B scam](#)  
[Monty Solomon via David Farber](#)
- [Mag-stripes on retail gift cards](#)  
[Tim Christman](#)
- [Luton schoolboy profits from Euro chaos](#)  
[Clive Page](#)
- [Another Euro surprise](#)  
[Otto Stolz](#)
- [A Web site about PC security asking to lower PC/browser security](#)  
[Koos van den Hout](#)
- [Other blunders on "secure" Web sites](#)  
[Skip La Fetra](#)
- [Re: Harvard admissions e-mail bounced by AOL spam filters](#)  
[Fredric L. Rice](#)
- [User Web habits tracked by some music-swapping programs](#)  
[NewsScan](#)
- [Kaiser Permanente exposes medical record numbers](#)  
[J Debert](#)
- [ATT ignores it's own privacy policy?](#)  
[J Debert](#)
- [Peoples Federal Savings Bank explains their interest calculations](#)  
[Jonathan Kamens](#)
- [Re: "Buffer Overflow" security problems](#)  
[Stephen Steel](#)
- [Re: "Buffer Overflow" security problems and PL/I](#)  
[Kelly Bert Manning](#)
- [Buffer overflows aren't the only issue](#)  
[Rex Black](#)
- [Separate I and D spaces](#)

[Mike Albaugh](#)

• [Info on RISKS \(comp.risks\)](#)

---

## ✈ Credit-card cloners' \$1B scam

David Farber <dave@farber.net>

Mon, 07 Jan 2002 20:07:25 -0500

Homemade machines costing about \$50 are being used to read credit-card mag-stripes, without having to steal the cards. The information is then e-mailed abroad, where cloned cards are fabricated. This has become a billion-dollar-a-year enterprise.

[PGN-ed from Monty Solomon's e-mail to Dave's IP, subtitled Terrorists, mobsters in on hacking racket, by William Sherman, \*NY Daily News\*  
[http://www.nydailynews.com/today/News\\_and\\_Views/City\\_Beat/a-137421.asp](http://www.nydailynews.com/today/News_and_Views/City_Beat/a-137421.asp)]

[The gadget was first demonstrated in maybe 1960s at Caltech as part of a demo on how poor the mag-striped credit cards were. In spite of that, they won. Dave]

---

## ✈ Mag-stripes on retail gift cards

Tim Christman <tjc@wavetech.net>

Sat, 29 Dec 2001 09:59:00 -0600

Here's a link to an article on MSNBC that I found interesting --  
[www.msnbc.com/news/598102.asp?0dm=C216T&cpl=1](http://www.msnbc.com/news/598102.asp?0dm=C216T&cpl=1)

Many retailers are replacing paper gift certificates with small plastic cards containing magnetic stripes, similar to credit cards. Ideally, the purchase of a gift card would result in a database being updated to reflect the balance associated with the card's unique account number.

Some retailers are using sequential account numbers and have no provisions to protect against a thief using a mag-stripe reader/writer to re-program a stolen card or small denomination card so that it matches the account number of a larger valued card purchased by someone else. Many retailers even provide a convenient 1-800 number so that the thief, knowing many valid account numbers, can "shop" for a card of significantly greater value.

The RISK: A form of fraud, difficult to trace, involving a minimal investment in equipment by the thief. Also note that the thief only requires the ability to query the back-end database (through the toll-free

number), not the ability to manipulate the records. Perhaps more ominously, the risk is angry family members who find a zero balance on their gift cards!

Solutions: One retailer, mentioned in the article, uses optical bar-coding which can't be re-encoded without defacing the card. Another follows a technique used by many credit card companies -- extra check digits are included in the mag-stripe that are not visible on the face of the card. It seems astounding that this isn't being done by all.

---

## ✈ Luton schoolboy profits from Euro chaos

Clive Page <Clive@page.demon.co.uk>  
*Sun, 6 Jan 2002 19:11:02 +0000*

I hope you won't mind another Euro-related story, but this one is rather charming. The facts are taken from my local newspaper, the \*Luton on Sunday\*, but the story made a brief appearance in some national papers.

Although the UK is one of the three European Union countries not to have adopted the Euro, many large retailers in the UK announced that they would accept them, but would give change in pounds sterling. Among these was the Debenhams chain of department stores. (Incidentally, I'm told that officially the plural of Euro is Euro, presumably to prevent language wars.)

Robert Sheilds, a 15-years old Luton schoolboy, decided he would like experience of using Euro, so he changed 10 pounds to Euro at a bank, and went on to his local branch of Debenhams to spend them. He found that they had programmed their tills as if there were 1.6 pounds to the Euro rather than 1.6 Euro to the pound, but none of the sales assistants was experienced enough to notice the error. So after his initial purchase, he still had more than 10 pounds in change. He tried to tell the store staff of their mistake, but they said the rate was programmed into the computer, and nobody had the authority to change it. So he carried on spending, and after two hours, ended up with 130 pounds of goods, and 20 pounds in cash. At this point the store manager asked him to leave, saying "I think you've had your fun". Richard then took a train to Bedford (about 20 miles away) to try his luck at another branch, but by this time staff had been alerted, and refused all Euro transactions.

---

## ✈ Another Euro surprise

Otto Stolz <Otto.Stolz@lh-iplanet.rz.uni-konstanz.de>  
*Tue, 08 Jan 2002 17:34:11 +0100*

Here is one more example of the unexpected implications a large project (such as the introduction of a new currency) can have. It is not a murderous risk, but you may find the story instructive, and perhaps amusing.

Today, I received an assessment from the local tax office. The amount due was the former amount converted from DM to EUR -- almost, but not exactly: it was rounded up to the nearest multiple of 0,1 EUR.

Thus, the new annual amount was no more a multiple of 4. As the amount is due by quarterly installments, the assessment told my to pay three equal amounts (at certain dates every year) and another amount, which is 0.02 EUR larger, at some other date.

Of course, my bank had already converted my standing remittance order from DM to EUR. However, this being not adequate, I tried to adapt it to the new tax assessment. (I dare not risk the trouble of owing anything to the tax office, not even 0,02 EUR, would you?)

It turned out that the bank is not prepared to handle a standing order of this type. I could have four annual orders instead, one per quarter. I preferred to do it the other way: I left my original order as it was, and placed a new order for 0,02 EUR (roughly 0,02 US\$) per year. I hope well that somebody at the tax office will be irritated with this extra paying.

The lesson to be learned: any change in a large, working system will have unexpected, possibly undesired, results. Be on your guard!

---

## ✄ A Web site about PC security asking to lower PC/browser security

Koos van den Hout <koos@kzdoos.xs4all.nl>

Mon, 7 Jan 2002 10:08:24 +0100

I received an e-mail this morning with an unknown .exe attachment which on inspection seemed to do something with registry keys. Since it doesn't look like any of the viruses I heard about recently I tried to look for it on <<http://www.mcafee.com/>>.

Therefor, I visited <<http://www.mcafee.com/>> first using Netscape 4.72 for Solaris (I use a Solaris workstation). The site shows a pop-up asking me to enable an ActiveX plug-in, but I might be able to use the site without it. The fact that I am using a different operating system for which an ActiveX plug-in isn't available at all has never crossed the mind of whoever designed that.

To top that, when I visit the site using Lynx 2.8.2 (a text-mode browser for Unix, quite popular with blind or near-blind Internet users) I just get a page asking me to enable scripting by LOWERING the 'Internet security'

setting on my Web browser. Never mind the fact that there are browsers for which there is no scripting and that it can be a decision made for security reasons. Literal text:

3. In the Internet Control Panel, Select the Security tab
4. Select the "Internet" zone
5. If the security level is set to "High"
  - a. Change the setting to "Medium" or click the "Reset" button for the Internet Zone

If McAfee wants to look like a company that sells products for 'Securing your PC' they might want to set up their Web site so I don't have to LOWER the security of my browser.

The security history of Javascript and ActiveX do not suggest to me that they are welcome on a 'Securing your PC' site.

[Genuine virus investigators interested in the mail with 'ASD.EXE' attachment should contact me privately]

Koos van den Hout koos@kzdoos.xs4all.nl <http://idefix.net/~koos/>

---

## ✂ Other blunders on "secure" Web sites

"Skip La Fetra" <Skip@LaFetra.com>  
Sat, 5 Jan 2002 14:15:07 -0800

In [RISKS-21.84](#), Jeffrey Mogul ("When a 'secure site' isn't") points to some "secure" sites which fail to properly implement https secure protocols.

In an incident from two years ago, my employer required use of an online form which required credit-card info for cards which were billed to employees. This "secure site" was provided by an external supplier. Naturally I checked for https use and browser "lock" icons.

All went well until the final confirmation screen. In addition to the "you have ordered zzzzz with credit card yyyyyy" expected, imagine my surprise when I noticed that the URL of the page contained ALL of my information:  
"https://securesite.com/verification.htm?name=3Dyyyyyy,CardNumber=3D12345=6789,ExpirationDate=3D12/31/2001" etc.  
Being part of the URL "address", this information (including my name, address, credit card number, and expiration date) was not protected, even though the page was sent using "https".

A discreet call to the webmaster for this site provided a quick reply -- that all was okay, and all pages were sent using "https".

A second call (and a CC to a very-high-ranking IT manager) explaining the difference between "PUT" and "GET" in forms processing produced a fix -- and an apology.

Moral: Even when the technology is secure, people can still blunder around it. The analogy which was effective in this case was talking to their IT engineers about the US postal system -- and pointing out that writing information on the outside of an envelope isn't secure even if the envelope itself is protected.

---

## ✈ Re: Harvard admissions e-mail bounced by AOL spam filters ([R-21.84](#))

"Fredric L. Rice" <[frice@skeptictank.org](mailto:frice@skeptictank.org)>  
*Tue, 08 Jan 2002 13:14:02*

I'll doubtlessly draw a lot of flack in my inbound e-mail for this comment yet what the hell: Harvard sent a lot of e-mail out to people who submitted entrance requests with an AOL return e-mail address and then AOL filtered them out as bulk spam. As much as many people hate to admit it -- whether it's deserved or not -- AOL users have a reputation in newsgroups approximately one step above that of WebTV users. "Get a real ISP and people will talk to you" is something I see in newsgroups from time to time.

I doubt that Harvard's admissions department looks at an AOL address and decides the applicant should be rejected based solely upon that fact but what about prospective employees? People in IT departments might wonder whether someone's using AOL because they're not Internet savy enough to figure out how to install, set up, configure and use a real ISP with real client software packages.

AOL is marketed toward the average smuck with a plug-it-in-and-it-will-just-work requirement. It doesn't take a genius to figure out how to use a real ISP with real servers and slients but AOL is targeted to people who don't want to read "Internet For Dummies."

---

## ✈ User Web habits tracked by some music-swapping programs

"NewsScan" <[newsscan@newsscan.com](mailto:newsscan@newsscan.com)>  
*Mon, 07 Jan 2002 09:23:26 -0700*

The Web surfing habits of people who used the LimeWire, Grokster and KaZaA music-sharing programs were surreptitiously tracked because those programs were linked to an online sweepstakes game called ClickTillUWin, in which players pick numbers and win cash prizes. The company that operates the

sweepstakes game says it told outside distributors to get users' permission before installing the software, but in these cases that action was not taken. The three companies have posted new versions of their software without the tracking component, and LimeWire has issued an apology. (AP/\*USA Today\*, 4 Jan 2002; NewsScan Daily, 7 January 2002)

<http://www.usatoday.com/life/cyber/tech/2002/01/04/limewire-tracking.htm>

---

## ✂ Kaiser Permanente exposes medical record numbers

j debert <jdebert@garlic.com>

Sat, 05 Jan 2002 23:52:37 -0800

Here's yet another example of how an organization fails to abide by it's own security policies:

Kaiser Permanente has a Web site for members at <http://www.kponline.org/> .

The first page here is the signon page, where one enters a medical record number and their region to enter the site.

A statement concerning online security can be seen at:

"<http://www.kponline.org/ns/signon/signonmember?view=Security>";  
<<http://www.kponline.org/ns/signon/signonmember?view=Security>> .

This statement indicates in the first paragraph that the medical record number will be sent via SSL:

### Signing On

You need to sign on using your Kaiser Medical Number.

This number will be transmitted using secure technology (SSL).

We need your Kaiser Medical Number before you get into the site for two main reasons:

(Note that this is the statement still in effect as of 1 Jan 2002.)

However no SSL connection is possible. Every attempt to obtain a secure connection gets redirected to the non-secure page.

The people in Kaiser's kponline service center seem to have no clue and no concern about this lapse. They say to disregard the security statement because it applies only to those already signed up for access which is not indicated in the security statement and cannot understand what the problem is. Pointing out that that is not what is stated just annoys them.

The service reps say that no one can use the medical record number to access personal information online. Seems like that's all they are concerned with. They also claim that there is no way a medical record number can be associated with a patient. I am fairly certain that these claims are easily proven false.

The RISKS are quite obvious but Kaiser seems oblivious to the obvious even when pointed out in detail.

---

## ATT ignores it's own privacy policy?

j debert <jdebert@garlic.com>  
Sat, 05 Jan 2002 23:23:56 -0800

Yet another example of how an organization ignores its own published privacy policy:

ATT allows customers to send form mail using SSL on their Web site. This is to keep their customer's info and the message private.

But their people include the entire message in plaintext e-mail messages sent in response defeating the purpose of the secure form.

Their privacy policy as published online essentially says that they will keep customer info private.

RISKS? What RISKS? TO customers? So? What's the problem???

---

## Peoples Federal Savings Bank explains their interest calculations

Jonathan Kamens <jik@kamens.brookline.ma.us>  
Sun, 23 Dec 2001 21:43:41 -0500

Well, it took five months of letters and contacting the local news media and several regulatory agencies, but I finally got Peoples to explain why their interest calculations for June 2001 differed from mine. So this message is the retraction I promised I would submit if Peoples proved to me that their interest calculations were correct.

(This, of course, does not change the fact that they stonewalled me for five months and caused me all sorts of other grief when they "upgraded" their computer systems in June.)

The technical explanation, for those of you who are interested.... In their old computer system, they calculated interest for the month on the second-to-last day of the month, using the ending balance for that day as the ending balance for the last day of the month as well. If in fact the ending balance changed on the last day of the month, a credit or debit was applied to the interest payment for the \*next\* month. My calculations of

what my interest payment should have been did not include this credit, and indeed \*could\* not include this credit because the bank never explained this part of their algorithm to me (despite my multiple requests for a precise explanation of how they were calculating interest).

On the bright side, their new computer system pays interest at the beginning of the month for the entire previous month, so this particular bit of brain-damage is gone. But I won't be staying with this bank for long enough to enjoy that particular "perk" -- would you stay with a bank whose officers either were incapable of explaining to you how they calculate interest, or simply refused to take the time to do so, until you pressured them about it for five months?

See <URL:[http://www.mit.edu/~jik/pfsb\\_problem/](http://www.mit.edu/~jik/pfsb_problem/)> for the whole story, including this latest installment.

Jonathan Kamens

---

## ✂ Re: "Buffer Overflow" security problems (Leichter, [RISKS-21.85](#))

Stephen Steel <steve.steel@kvs.com>

Mon, 7 Jan 2002 19:12:39 -0500

The primary problem here is not the C language, but the associated standard library, because the library is responsible for a lot of the C/C++ programming culture. Almost every book on C programming had lots of examples using `sprintf()`, `strcpy()` and other buffer overflow prone functions. And programmers took these examples to heart, duplicating them in the programming interfaces they wrote.

If the topic of buffer overflows came up, then `strncpy()` would probably be mentioned. What a fine example this was for the beginning programmer: it wouldn't overwrite the destination buffer if called correctly, but the copy of the original string in the buffer had an unbounded length! (since the copy would not be properly NUL terminated if the source string was as long or longer than the buffer size).

Its a great pity the first C standards didn't provide two variants of the standard library and a standard means of selecting which variant would be used. Safe versions of the problematic functions would be include in both variants, and the recommended variant library would have omitted the unsafe functions completely (for completely new code).

Stephen C. Steel <stephen.steel@kvs.com>

## ✂Re: "Buffer Overflow" security problems and PL/I

Kelly Bert Manning <bo774@freenet.carleton.ca>  
Mon, 7 Jan 2002 21:54:47 -0500 (EST)

PL/I also supports string subscript range checking, in addition to Array Bounds checking, but in working with PL/I since 1973 I've never seen a site that had them as the site default. The site I currently work with runs at 100% processing capacity from 07:00 to 23:00 every day. OTOH, they feel that DB2 is the way to go even though IMS still beats DB2 by at least 2:1, so perhaps it would be worth giving this a try as the site

At the moment I can't recall whether a protection exception or a data exception is the most common symptom, but I've got it down to the point where I can quote the PL/I manual section advice about adding a Subscript and Array bound Check prefix in my sleep for "unidentified routine malfunction" types of errors when on call programmers give up and ask for DB Admin advice.

[publibz.boulder.ibm.com/cgi-bin/bookmgr\\_OS390/BOOKS/ceeal110/2.4.1.7?](http://publibz.boulder.ibm.com/cgi-bin/bookmgr_OS390/BOOKS/ceeal110/2.4.1.7?ACTION=MATCHES&REQUEST=subscriptrange&TYPE=FUZZY&searchTopic=TOPIC&searchText=TEXT&searchIndex=INDEX&rank=RANK&ScrollTOP=FIRSTHIT#FIRSTHIT)

[ACTION=MATCHES&REQUEST=subscriptrange&TYPE=FUZZY&searchTopic=TOPIC&searchText=TEXT&searchIndex=INDEX&rank=RANK&ScrollTOP=FIRSTHIT#FIRSTHIT](http://publibz.boulder.ibm.com/cgi-bin/bookmgr_OS390/BOOKS/ceeal110/2.4.1.7?ACTION=MATCHES&REQUEST=subscriptrange&TYPE=FUZZY&searchTopic=TOPIC&searchText=TEXT&searchIndex=INDEX&rank=RANK&ScrollTOP=FIRSTHIT#FIRSTHIT)

It rarely shows up in that overt form. I'm more concerned about it happening quietly without ringing alarm bells. BTW, in the only major program where I ever had to worry about array overflow(why not use a DB instead) I made the array CONTROLLED with a REFER clause and checked the array size explicitly, allocating a new larger array and printing and warning message if I reached the array size limit.

It is always interesting to compare the confidence with which programmers state that they don't feel they have an Array bound problem with their quite manner when they get back to me with confirmation that adding the stringrange and subscriptrange checks zeroed in on the problem.

---

## ✂Buffer overflows aren't the only issue

Rex Black <rexblack@ix.netcom.com>  
Mon, 07 Jan 2002 21:35:35 -0600

As a long-time practitioner of software testing, let me mention that, while buffer overflows are commonly exploited for security breaches, plenty of software quality problems--some of which are quite risky to the users--arise from other causes. Just off the top of my head, I can spout off the following unforgivable "buggy software" stories, none of which have anything to do with buffer overflows as far as I can tell:

\* An expense reporting program, QuickXPense, that didn't have any data

quality bugs at all...at least until the operating system crashed. (Gee, what are the odds of that?) Once the OS did crash, the file was randomly corrupted, and the corruption cascaded with subsequent use, so ultimately the entire expense report file was garbage. The vendor's technical support staff was aware of the problem, but rather than a patch or a file report utility, they suggested that I "e-mail your file and we'll fix it." Well, sure, there's nothing private or personal in that file.

\* The fact that some PowerPoint presentation files, if corrupted--by, say, the computer going into power-saving hibernation at just the wrong time--in as much as a single bit in some cases, can become totally unreadable by the program. (See the first and last bullet for ways this might happen.) Microsoft knows about this bug, but they choose not to include recovery utilities in their applications. Instead, after a \$100 paid support call, they send you to a software developer--who would be called a "highwayman" a couple centuries ago--who charges \$400 for his recovery tool. Talk about turning the incompetence of others into a business opportunity!

\* The Windows NT network driver that came with a 3Com network card which, on two out of three boots, is unable to see the network. No diagnostic messages come up. Cold booting the system until communications are re-established is the only cure.

\* The automatic update software in my Toshiba laptop that recently "upgraded" the drivers for the built-in Xircom MPCIE modem--without prompting me--which resulted in the loss of all modem definitions in my Windows "Device Manager". (Device mismanager?) I wasted an entire day trying to get the drivers reloaded. Toshiba's technical support was worse than clueless, having me try the same thing over and over until the batteries on my cell phone died, ending the call. Ultimately I had to go out and buy a new modem, which also turned out to solve a bunch of connection problems I had, indicating that the buggy setup problem was only the tip of the iceberg, quality-wise, with this modem.

\* The Lexmark printer I bought that didn't say anything in the manuals or installation process about the fact that you couldn't install it on a networked PC and access it from other systems on the network. After a few hours of trying, I e-mailed tech support, only to get response that boiled down to, "Oh, yeah, you can't do that." Oh, really? Why can't I do that? I have a twelve-year-old Epson dot matrix printer that was built before anyone had a small office network. I can share that printer just fine with every computer on my network. This whiz-bang color printer-scanner-copier that I bought in the day of ubiquitous small office/home office/home computer networking can't be shared with other computers? Pshaw!

\* The daily (or more often) crash that my Windows Me laptop computer subjects me to, generally without warning, usually losing a good fifteen minutes worth of work. I guess I should learn to save every thirty seconds?

If experienced people like me have problems like this, imagine the average computer user who has no idea whatsoever about what is going on when her system screws up. And why should they have to understand a computer to use them? (Don Norman, in his book *\*The Invisible Computer\**, discusses this

situation at length.) Ultimately, a computer is a tool, nothing more, nothing less. I think we have a long way to go before we can claim levels of quality consistent with what the makers of almost any other tool could claim.

Rex Black, Principal, Rex Black Consulting Services, Inc., 31520 Beck Road  
Bulverde, TX 78163 USA +1 (830) 438-4830 [www.rexblackconsulting.com](http://www.rexblackconsulting.com)

---

## ✂ Separate I and D spaces (Re: Buffer overflows, Baker, [RISKS-21.85](#))

Mike Albaugh <[albaugh@spies.com](mailto:albaugh@spies.com)>

Mon, 7 Jan 2002 15:22:45 -0800 (PST)

[This feels like my days reading comp.programming (Been "clean and sober" off Usenet for over a year now :- ) MEA ]

... As someone who, until very recently, wrote primarily code that was executed from ROM, I need to point out that "corrupting running code" is not needed. If one can corrupt the subroutine return-address (normally `_part_` of a buffer-overflow attack), one can point it wherever one wishes. If a sufficiently dangerous set of instructions (or bytes that could be interpreted as instructions) already exists in the "instruction memory", one can do the intended mischief.

As for Henry's assertion that such devices are "more vulnerable" because "nobody bothers to run virus-checking software on them", I think this exhibits touching faith in anti-virus authors and a mis-understanding of the most common recent viruses. Outlook could be in ROM and "Execute Only" (No-Read) and I still would have gotten a mailbox full of mail whose subject I won't include so this copy of RISKS will get through :- ) Buffer-overflows are indeed examples of shoddy programming practices, but they are hardly the most popular vulnerability. People who leave their doors open need not fret overly about the quality of their locks.



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 21: Issue 87

**Saturday 19 January 2002**

## Contents

- [Exploding chips: Would you like to be fried with that?](#)  
[Rob Slade](#)
- [Hospital tells elderly men they're pregnant](#)  
[Arthur Goldstein](#)
- [Automated Debit: "There's nothing we can do to stop it."](#)  
[Carl Fink](#)
- [Even unscientific elections get rigged](#)  
[Jeremy Epstein](#)
- [The risks of standards and validators](#)  
[Lindsay Marshall](#)
- [Buffer overflows and other stupidities](#)  
[Earl Boebert](#)
- [Windows update server glitch](#)  
[Mike Hogsett](#)
- [An outrageous violation of privacy](#)  
[Fred Cohen](#)
- [Risks of Internet Reconfigurable Logic](#)  
[John Gilliver](#)
- [Linked DMV databases and biometrics on driver's licenses](#)  
[Ben Rosengart](#)

- [Facial recognition technology doesn't work](#)  
[Nick Brown](#)
  - [Honolulu speed camera risk: mainly human error](#)  
[Dan Birchall](#)
  - [AOL Buddy-Hole fix has backdoor](#)  
[Robert Andrews](#)
  - [Reinventing snake oil: compression](#)  
[Jeremy Epstein](#)
  - [Re: Airplane takes off without pilot](#)  
[Paul Nelson](#)
  - [Re: Software glitch grounds new Nikon camera](#)  
[Nickee Sanders](#)
  - [Re: Kaiser Permanente exposes medical record numbers](#)  
[Geoff Kuenning](#)
  - [Re: ING bank debits wrong sum from accounts](#)  
[Paul van Keep](#)
  - [REVIEW: "Counter Hack", Ed Skoulis](#)  
[Rob Slade](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

## ✶ **Exploding chips: Would you like to be fried with that?**

Rob Slade <rslade@sprint.ca>  
Thu, 17 Jan 2002 08:58:01 -0800

From NewsScan Daily, 17 January 2002:

```
> EXPLODING CHIPS COULD FOIL THIEVES
> Researchers at the University of California in San Diego have
developed a
> way to blow up silicon chips using an electric signal --
```

Now, at this point I was willing to dismiss this as the stuff of fiction.

You all know how computers in books and movies always "blow up real good"

when the bad guy plants a virus or something in them. However:

- > an innovation that could be used to fry electronic circuitry in devices
- > after they're stolen or fall into the wrong hands. The American spy plane
- > that was impounded in China last year is an example where such technology
- > would have proven handy in destroying its secret electronics systems.

OK, this make a bit more sense. Obviously these are chips that are specifically designed to blow up once they receive a certain signal.

At this point, though, you start to think about what kind of signal that could be. And, could it be counterfeited?

- > Similarly, if a cell phone were stolen, the owner could alert the wireless
- > carrier, which would send a signal to trigger a small explosion in the
- > phone's chip, rendering it useless. The techniques uses a small amount of
- > the oxidizing chemical gadolinium nitrate applied to a porous silicon
- > wafer. (New Scientist 16 Jan 2002)
- > <http://www.newscientist.com/news/news.jsp?id=ns99991795>

OK, I am definitely certain that, if I need to get a new cell phone from now on, I am *\*definitely\** not going to carry it in my pants pocket. The RISKS, as have been frequently noted here, are obvious.

(If we could get them to use those chips in pacemakers, wouldn't that just make a killer application, Peter?)

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>

[I normally delete all trailer quote. But this one from another message

from Rob is rather fascinating:

A modern US Navy cruiser now requires 26 tons of manuals.

This is enough to affect the vessel's performance.

-- `New Scientist' article on the paperless office

PGN]

---

## ✶ Hospital tells elderly men they're pregnant

<arthur.goldstein@att.net>

*Fri, 11 Jan 2002 04:19:19 +0000*

The Chesterfield and North Derbyshire Royal Hospital admitted on 10 Jan that

it had mistakenly sent computer generated letters to 30 patients, including

six elderly men, telling them they were pregnant. The system operator was

blamed for choosing the wrong option (instead of informing them that their

operations had been postponed). [Reuters, 10 Jan 2002, PGN-ed]

<http://news.excite.com/article/id/65168>

[|oddlyenough|01-10-2002::11:30|reuters.html](http://oddlyenough|01-10-2002::11:30|reuters.html) [SPLIT URL]

---

## ✶ Automated Debit: "There's nothing we can do to stop it."

Carl Fink <carl@fink.to>

*Wed, 16 Jan 2002 14:02:08 -0500*

A Georgetown, TX man who had arranged for his water bill to be automatically debited from his bank account alertly noticed that his monthly bill was for over \$21,000. (If he hadn't noticed, the debit would have happened, causing him to bounce multiple checks before the error was corrected.) When he told the city of the problem, "They said there was absolutely nothing they could do to stop the automated debit, and it was out of their hands." Their solution was to send a city employee with a check for \$21,000 to reimburse their customer!

[http://www.austin360.com/statesman/editions/tuesday/metro\\_state\\_1.html](http://www.austin360.com/statesman/editions/tuesday/metro_state_1.html)

Risks? Lack of sanity checking on a new billing system springs to mind. Lack of any way to correct errors is also quite prominent.

Carl Fink, Manager, Dueling Modems Computer Forum <http://dm.net/> carlf@dm.net

---

## **✶ Even unscientific elections get rigged**

"Jeremy Epstein" <jepstein@webmethods.com>  
*Wed, 9 Jan 2002 16:28:26 -0500*

ZDNet is doing a poll on whether J2EE or .NET is more important for Web services. Although it's a totally unscientific poll, they've set things up to try to detect (and stop) ballot stuffing. It seems that Microsoft hasn't understood the concept, and employees are trying to vote repeatedly,

including automated voting.

<http://news.zdnet.co.uk/story/0,,t269-s2102244,00.html>

The risk of believing unscientific polls is nothing new, but the combination of electronic polls that can be stuffed with the herd mentality that may influence buying greatly increases the risks.

[\*The Register\* noted that 21.5% of the respondents said they would

use .Net, 46% Java -- until a surge of votes came in from microsoft.com,

some of which were apparently stimulated by internal MS e-mail saying

"PLEASE STOP AND VOTE FOR .NET!". PGN]

---

## ⚡ The risks of standards and validators

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

*Fri, 11 Jan 2002 13:16:36 -0000*

This week I ran a page of the RISKS Web site through the W3 html validator,

as I do on a regular basis -- it keeps me clean and legal. It complained

that I didn't have a charset specification, so I added one as it suggested.

This appears to cause some netscape 4.7 browsers some problems -- I had

complaints that the text was vanishingly small, and also that it was vastly

increased in size. Presumably a typeface selection that is hard-wired

somewhere, and that nobody is told about. Anyway, I've taken out the

charset setting for the moment.

<http://catless.ncl.ac.uk/Lindsay>

[Lindsay runs our UK redistribution and the excellent RISKS Web site --

for both of which I am most grateful. I'm delighted to take the opportunity to thank him once again! PGN]

---

## ✶ Buffer overflows and other stupidities

Earl Boebert <boebert@swcp.com>

*Mon, 14 Jan 2002 10:07:55 -0700*

"I used to be disgusted, now I try to be amused." -- Elvis Costello

"What a stupid robot." -- Marvin the Paranoid Android

In my view, attempts to close the buffer overflow vulnerability through software or compiler tricks are doomed to one degree of failure or another because you're trying to program around a stupid processor design. Certain contemporary processors actually host a Pantheon of stupidities, consisting of a Greater Stupidity and two handmaiden Lesser Stupidities.

Greater Stupidity: Read access implying execute access. Any piece of data that the processor can be tricked into loading into the command register immediately becomes code. This is a stupidity of such breadth and depth that it comes with an event horizon.

Lesser Stupidity I: Segmented addressing that isn't. Let's say you have an addressing scheme consisting of segment number plus offset. This

raises the question of what to do when, in executing code, block moves, etc., the offset gets counted up to maximum length plus one. Smart answer: take a fault. Dumb answer: set offset to zero and count up one in segment number.

Lesser Stupidity II: Brain-dead stack design. If you enumerate the design space of dynamic storage management, you may realize that one actually has to \*work\* to produce a stack design so dumb that overflow attacks are possible. Here are four classes of designs that are immune to the vulnerability:

1. Descriptor stacks. The only thing that goes in the stack are addresses, preferably with a bounds value attached. Overflow a buffer and at worst you clobber the heap. Penalty: one level of indirection, which (The Horror! The Horror!) may cause your dancing pigs to dance slower than the other guy's. Possibility: can be fitted transparently to existing processor designs, assuming anybody cared.

2. Stack per protection domain. This assumes you can find the perimeters of your protection domains. Also slows down dancing pig displays because of copying parameters from stack to stack.

3. Separate control and data stacks. CALL/RETURN works the control stack, PUSH/POP works the data stack. Doh.

4. Error-checking stacks. A whole raft of options, including "shadow stacks" with checksums, return addresses protected with trap bits, etc. etc.

So, if it's all so straightforward and well known, why hasn't some vendor or other fixed it? Answer: the dancing pigs have won.

[Ah, yes. Earl is tacitly recalling the good old days of Multics

(beginning in 1965) and its progenies (SRI's object-oriented Provably

Secure Operating System design 1973--1980, and the Honeywell/Secure

Computing Corporation type-enforced systems), all of which took care of

this problem and so many others so long ago. But with today's badly

designed bloatware, the dancing pigs are increasingly becoming 700-pound

porkers that can barely move around the pigsty without massive memory

and processing power, and whose pigpen could not even contain them if

they were in reality Trojan pigs. PGN]

---

## ⚡ Windows update server glitch

Mike Hogsett <hogsett@csl.sri.com>

Tue, 15 Jan 2002 14:48:14 -0800

A glitch in Microsoft's server software has left some users unable to download important security patches and other fixes for Windows software since last Thursday.

<http://www.cnn.com/2002/TECH/internet/01/15/microsoft.security.server.ap/index.html>

<http://www.cnn.com/2002/TECH/internet/01/15/microsoft.security>.

[server.ap/index.html](http://server.ap/index.html)

[microsoft.security.server.ap/index.html](http://microsoft.security.server.ap/index.html) [SPLIT]

---

## **✶ An outrageous violation of privacy**

Fred Cohen <fc@all.net>

*Sun, 13 Jan 2002 10:27:20 -0800 (PST)*

I just saw a piece on MSNBC where they prominently featured the face of a man who helped someone out of the WTC on 11 Sep 2001 -- and just because they don't know who the man is, they have created a composite picture of him and posted him as if he were a wanted man on the national news.

Now I understand their desire to make human interest stories go, but I think it is outrageous to take the image of a person and smear it all over national TV, creating a manhunt for someone, when all the person did was to help someone else out in a public place.

If I were this man, I would sue them for as much as I could get and do all I could to try to recover what semblance of privacy I might barely still have left after being exposed on national TV without my permission.

Is this all we have left of our privacy?

Fred Cohen <http://all.net/> Fred Cohen & Associates tel/fax:925-454-0171

Sandia National Laboratories 1-925-294-2087 University of New Haven

## **⚡ Risks of Internet Reconfigurable Logic**

<john.gilliver@baesystems.com>  
*Tue, 08 Jan 2002 16:40:35 +0000*

... "For example, IRL (Internet Reconfigurable Logic) means that a new design can be sent to an FPGA in any system based on its IP address."

(From Robert Green, Strategic Solutions Marketing with Xilinx Ltd., in

"Electronic Product Design" December 2001. Xilinx is a big manufacturer of FPGAs.)

For those unfamiliar with the term, FPGA stands for field-programmable logic array: many modern designs are built using these devices, which replace tens or hundreds of thousands of gates of hard-wired logic.

The RISKS involved are left as an exercise to the readers ...

J. P. Gilliver, BAE SYSTEMS Advanced Technology Centre,  
West Hanningfield Road, GREAT BADDOW, Essex, CM2 8HN, UK +44  
1245 242133

---

## **⚡ Linked DMV databases and biometrics on driver's licenses**

Ben Rosengart <ben+risks@narcissus.net>  
*Wed, 9 Jan 2002 17:38:14 -0500*

\*Time Magazine\* is reporting that the federal Department of Transportation, by instruction of the Congress, is working to link together the

states'  
driver databases, and also to introduce biometric security on  
drivers'  
licenses.

<http://www.time.com/time/nation/article/0,8599,191857,00.html>

RISKS include false arrest due to database screwups, abuse for  
personal  
reasons by government personnel, abuse by the government itself,  
all the  
RISKS known to be associated with biometrics, disclosure of the  
databases to  
the public, and probably much, much more.

---

## ✶ Facial recognition technology doesn't work

Nick Brown <Nick.BROWN@coe.int>

*Wed, 9 Jan 2002 11:38:39 +0100*

An article by the ACLU at

[http://www.aclu.org/issues/privacy/drawing\\_blank.pdf](http://www.aclu.org/issues/privacy/drawing_blank.pdf) reveals  
that a  
highly-publicised facial recognition system has been quietly  
dropped by law  
enforcement officials in Tampa, Florida, following a large  
number of false  
positives (including males identified as females, and vice  
versa) and a  
total of zero matches against known criminals, leading to zero  
arrests.

Aside from the already-discussed civil liberties RISKS of such  
systems, it  
seems we need to add the possibility that the taxpayers may not  
be getting  
value for money, with or without their knowledge (the withdrawal  
of this

kind of thing tends to be done with rather less media coverage than its introduction). One wonders if this will have any effect on plans to introduce such systems into airports to "detect" terrorists.

Nick Brown, Strasbourg, France

---

## ✶ Honolulu speed camera risk: mainly human error

Dan Birchall <djb@nospam.danbirchall.com>

*Wed, 9 Jan 2002 22:52:58 -1000*

After much debate, and general wailing and gnashing of teeth from those who like to drive fast, the powers that be here in Honolulu have a private contractor operating cameras to photograph vehicles which speed or run red lights. After the license number, time, and location of the violation are verified, a citation is mailed.

In their first day of operation, the cameras caught 927 speeders.  
<http://starbulletin.com/2002/01/03/news/index1.html>

However, more than 80% were unenforceable due to human errors in operation of the cameras - poor aim, inaccurate location recording, etc.  
<http://starbulletin.com/2002/01/08/news/index4.html>

On the bright side, people do seem to be speeding less since the cameras started working.

<http://danbirchall.com/>

## ⚡ AOL Buddy-Hole fix has backdoor

"Robert Andrews @ PrivacyExposed.com" <Robert@PrivacyExposed.com>

*Wed, 9 Jan 2002 12:19:10 -0400*

"A member of w00w00, the security enthusiasts who first reported the AOL

Instant Messenger (AIM) games request vulnerability, has alerted users that

a fix the group recommends has its own backdoor. Apparently, the AIM Filter

by Robbie Saunders which w00w00 had recommended is infected, group member

Jordan Ritter disclosed on the Bugtraq mailing list late Tuesday. "At the

time, Robbie Saunders' AIM Filter seemed like a nice temporary solution.

Unfortunately, it instead produces cash-paid click-throughs over time

intervals and contains backdoor code combined with basic obfuscation to

divulge system information and launch several Web browsers to porn sites,"

Ritter wrote." [...] Thomas C Greene, \*The Register\*

<http://www.theregister.co.uk/content/4/23596.html>

---

## ⚡ Reinventing snake oil: compression

"Jeremy Epstein" <jepstein@webmethods.com>

*Wed, 9 Jan 2002 16:13:31 -0500*

Snake oil is on the rise. Latest to join the fray is Zeosync (www.zeosync.com), which announced on 7 Jan 2002 that they have new

algorithms that can provide 100:1 lossless data compression over

"practically random" data. (What they mean by "practically" isn't defined.)

Lots of criticism and proofs that it's impossible in Slashdot [slashdot.org/article.pl?sid=02/01/08/137246&mode=thread](http://slashdot.org/article.pl?sid=02/01/08/137246&mode=thread)

and elsewhere. So far the algorithms haven't been given, except to provide

the single longest stream of buzzwords I've seen in a long time. The one

part that says it might not be 100% snake oil is that they have a Fields'

Prize winner as one of the participants.

The risk here is that they've added enough buzzwords to the announcement

that some people might actually believe it. The media doesn't seem very

skeptical, which they should be. Reuters quoted David Hill, an analyst with

Aberdeen Group as saying "Either this research is the next 'Cold Fusion'

scam that dies away or it's the foundation for a Nobel Prize. I don't have

an answer to which one it is yet." Others have been much more willing to

figure out which way it's going. Remember the 1999 story about the

16-year-old Irish girl whose new form of cryptography would revolutionize

the world?

---

## ✶ Re: Airplane takes off without pilot (Klein, [RISKS-21.84](#))

<pnelson@sauer-danfoss.com>

Mon, 7 Jan 2002 15:20:53 -0600

There are many aircraft which have no starters (or electrical system, for

that matter)- commonly antique or classic small, one- or two-

place planes  
like the 1947 Aeronca Champ that was the subject of this item.  
There are  
well-known safety precautions which go along with starting them-  
one of the  
oldest is that there should be someone in the cockpit with feet  
on the  
brakes, operating the magneto switches and throttle while a  
second person  
"props" the plane to start it. (The classic shouts "CLEAR!",  
"CONTACT!",  
"SWITCH OFF!", "BRAKES", "THROTTLE BACK AND CRACKED!" come to  
mind.)

If a plane like this is to be started by one person, the accepted  
precaution is to tie the tailwheel to a stationary object, turn  
the fuel  
OFF so that only the small amount in the carburetor bowl is  
available, and  
then make CERTAIN that the throttle is only cracked open a small  
amount.  
I've started my 1946 Cessna 140 in this manner many times when  
the battery  
happened to be run down.

All that being said, incidents like this still happen when  
people try to  
take shortcuts. It shouldn't have happened!

Paul Nelson, Senior Engineer, Sauer-Danfoss Company, Ames, IA  
515-239-6614

---

**✶ Re: Software glitch grounds new Nikon camera (Gillett, [RISKS-21.85](#))**

Nickee Sanders <njs@ihug.co.nz>  
Wed, 9 Jan 2002 12:10:32 +1300

Our first digicam was also a Kodak. When the battery voltage was low enough (and it happened suddenly), the camera would simply stop responding to \*any\* user actions whatsoever. It didn't even do a power down. The only way to clear this condition was to take the batteries out for a number of hours; after this, on insertion of fresh batteries, the camera would power down and then could be powered up again.

The first time this happened it was pretty scary. One minute we were snapping away; the next minute the camera was frozen, with the lens fully extended (and thus the lens cap wouldn't stay on it). The local service reps knew nothing of this error condition and could only offer to send it to Australia (from New Zealand) for servicing, which would take several weeks. We figured out by trial and error how to solve it ourselves.

Nickee Sanders, Auckland, New Zealand

---

## **✶ Re: Kaiser Permanente exposes medical record numbers (Debert, [R-21.86](#))**

Geoff Kuenning <geoff@cs.hmc.edu>  
*Mon, 14 Jan 2002 13:09:28 -0800*

J. Debert writes about an insecure Web page at <http://www.kponline.org>.

It happens that my best friend works for Kaiser Permanente's IT department, so I forwarded the message to her. As a result of discussions

and  
exploration, I think that the alleged risk does not in fact  
exist.

The claim was that medical-record numbers were being exposed  
during the  
signon process. However, in viewing the source of the  
referenced Web page,  
it appears that the "sign on" button makes an https (SSL)  
connection. Thus,  
although the "padlock" icon in the browser is unlocked, anything  
sent from  
that page is in fact sent using SSL.

I have recommended that Kaiser change their main page so that it  
forwards  
the browser to an SSL equivalent, solely so that the padlock  
icon will  
appear locked.

I think that the true RISK is not in Kaiser's Web page, but  
rather in the  
browser. The "padlock" icon reflects not whether the page SENDS  
information  
securely, but rather the fact that the page was FETCHED  
securely. This  
disconnect between what is shown and what is expected has been  
raised  
recently by Jeff Mogul in the converse direction: a page that  
had the  
padlock proceeded to send information insecurely.

The first problem (apparently insecure page is actually secure)  
can be  
patched around with the forwarding kludge I mentioned above.  
The second can  
be handled by the user to some extent (certain browser settings  
can warn you  
when you transition from a secure page to an insecure one).  
However, the  
true problem is in browser design. The "padlock" icon should be  
associated  
with a LINK, not a page. Regardless of how it was fetched, if a

page

contains both secure and insecure links, the lock should be shown as unlocked and should lock only when you mouse over a secure link. Only if all outgoing links from a page are secure should the padlock be permanently displayed in its locked form.

Geoff Kuenning    geoff@cs.hmc.edu    <http://www.cs.hmc.edu/~geoff/>

---

## ✶ Re: ING bank debits wrong sum from accounts

Paul van Keep <paul@sumatra.nl>  
*Wed, 9 Jan 2002 11:04:45 +0100*

Several people have pointed out that I was wrong in my statement about disproving a 10000 euro cash withdrawal would be tough. Banks have a sane upper limit on the amount of cash you can withdraw from an ATM, even at your own branch. That limit is somewhere below 2000 euro. A 10000 euro ATM transaction is therefore totally impossible.

Paul van Keep

---

## ✶ REVIEW: "Counter Hack", Ed Skoullis

Rob Slade <rslade@sprint.ca>  
*Mon, 14 Jan 2002 07:34:47 -0800*

BKCNTTRHK.RVW 20011023

"Counter Hack", Ed Skoullis, 2002, 0-13-033273-9, U\$49.99/C\$75.00  
%A Ed Skoullis  
%C One Lake St., Upper Saddle River, NJ 07458  
%D 2002  
%G 0-13-033273-9  
%I Prentice Hall  
%O U\$49.99/C\$75.00 800-576-3800 416-293-3621  
%P 564 p.  
%T "Counter Hack"

Chapter one, as in many texts, is an introduction to the book, but is unusually important in this case. First, Skoullis lays out the philosophy behind the work. While the text of the book does concentrate on attacks, the author points out that invaders already have other sources of information. Further, Skoullis proposes that a detailed, complete, and integrated examination of representative samples of classes of attacks will provide an outline of defensive measures that can protect against a wide variety of assaults.

A second point in this introduction is a brief examination of the character of attackers. Skoullis does point out that those who attempt to penetrate computer and communications security do so from a diversity of motivations and skill levels. However, he does tend to overstress the participation of "professional hackers," proposing that industrial espionage, terrorism, and organized computer crime activities are common. Certainly such campaigns may become common, making the need for pre-planning even more important, but the vast majority of endeavors we are seeing at present are

amateur efforts.

Finally, the introduction recommends the establishment of a computer security test laboratory, which is an excellent idea for any large corporation, but probably is not within the financial, personnel, or educational reach of even medium sized businesses.

Chapter two provides a background in TCP/IP for the purposes of discussing networking offence and defence. There are frequent forward references to later sections of the book that deal with network attacks. The material could, however, have been condensed somewhat to emphasize those aspects of the protocols that are closely related to security. UNIX and Windows (NT and 2000) are similarly covered in chapters three and four, and, again, the text could be tightened up by focusing on safety factors.

Chapter five points out the ways in which people can obtain data in order to direct and mount an attack. While the content is informative, and there are a few suggestions for restricting the release of such intelligence, the defensive value of the text is limited. The information gathering process continues in chapter six with war dialling and port scanning. Defences against application and operating system attacks are covered a bit better than in most "hacking" books (there are descriptions of buffer overflow detection tools), but the protective value of chapter seven is still questionable. Chapter eight examines network sniffing, scanning, spoofing, and hijacking. Denial of service is covered well in chapter

nine. Various examples of malware are described in chapter ten. Chapter eleven deals with the means used to hide an attack.

A number of scenarios are created in chapter twelve. Chapter thirteen describes some resources for keeping up with the latest computer vulnerabilities.

Recently there has been a flood of books to the security marketplace, all based on the premise that if you know how to attack a system, you will know how to defend it. Skoulis has done a better job than most, but the thesis is still unproven. Yes, knowledge of the details of an attack does help you fine tune your defence. Yes, providing specifics of an example of a class of attacks does help you consider a protective mechanism that might work against a whole class. Yes, Skoulis does recommend safeguards for most of the attacks listed. But taking a crowbar to a padlock still doesn't teach you locksmith skills.

copyright Robert M. Slade, 2001    BKCNTTRHK.RVW    20011023  
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 21: Issue 88**

**Tuesday 22 January 2002**

## Contents

- [Bulgarian parliament against weight loss](#)  
[Jonathan Larmour](#)
- [Pope loves Internet, but wants "anti-depravity regulation"](#)  
[Declan McCullagh](#)
- [Unshredders](#)  
[PGN](#)
- [Newspaper archives](#)  
[Roger Needham](#)
- [Virginia county recalls student laptops](#)  
[NewsScan](#)
- [Software uncovers e-mail untruths](#)  
[NewsScan](#)
- [Georgia Tech anti-cheating software](#)  
[Walter Roberson](#)
- [Anthrax mail irradiation can affect electronic devices in postal mail](#)  
[Thomas Dzubin](#)
- [Health insurer computer changes delay payments...](#)  
[Don Mackie](#)
- [Excel cut-and-pasting behaviour](#)  
[Geoffrey Brent](#)

- [Lotus Notes silently losing data](#)  
[Erling Kristiansen](#)
  - [Woman says telephone makes unsolicited calls](#)  
[Carl Fink](#)
  - [Answering machine provides door entry code](#)  
[Benjamin Elijah Griffin](#)
  - [Microsoft using predictable passwords for Passport?](#)  
[Rodger Donaldson](#)
  - [Re: Other blunders](#)  
[Brett](#)
  - [Re: Kaiser Permanente exposes medical record numbers](#)  
[George C. Kaplan](#)
  - [Re: Bogus dates for McAfee virus alerts](#)  
[David Blakey](#)
  - [Re: AOL's spam filters](#)  
[Jay Levitt](#)
  - [Call for Participation Open Source Software Development Workshop](#)  
[Cliff Jones](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

## 🚀 Bulgarian parliament against weight loss

Jonathan Larmour <jlarmour@redhat.com>

*Tue, 22 Jan 2002 21:46:47 +0000*

According to the (UK) Daily Telegraph, the Bulgarian parliament has a system of electronic voting, whereby Members vote with cards using a machine attached to their seats.

Unfortunately, the designers didn't anticipate that more enterprising MPs would swap seats and also slip a voting card into absent neighbouring colleague's machines!

I would have thought the (surely obvious) solution to this problem would have been personalised cards. But instead the parliament is introducing weighing scales set into the seat so that the votes will not be counted unless the weight of whoever is sitting there matches that of the MP whose seat it is.

The risks of the initial design are obvious. There appears to have been absolutely no consideration of security or checking whatsoever. The risks of the "solution" are more interesting, including the possibility of preventing someone voting in the afternoon by making sure they have a large lunch!

---

## 🔥 Pope loves Internet, but wants "anti-depravity regulation"

Declan McCullagh <declan@well.com>  
*Tue, 22 Jan 2002 14:11:58 -0800 (PST)*

Pope John Paul says that the Internet caters to the best and worst of human nature and needs regulation to stop depravity flooding cyberspace. He warned that while it offered access to immense knowledge, the Internet did not necessarily provide wisdom and could easily be perverted to demean human dignity. ``Despite its enormous potential for good, some of the degrading and damaging ways the Internet can be used are already obvious to all. Public authorities surely have a responsibility to guarantee that this

marvelous instrument serves the common good and does not become a source of harm.' Although the Pope does not have an e-mail address, the Vatican has an active Web site ([www.vatican.va](http://www.vatican.va)) and the Church is reportedly searching for a patron saint of Internet users.

[Source: Pope Says Internet 'Wonderful' but Needs Regulating, by Crispian

Balmer 22 Jan 2002, via Reuters; PGN-ed after DM's snipping]  
[http://dailynews.yahoo.com/hix/nm/20020122/wr/pope\\_internet\\_dc\\_1.html](http://dailynews.yahoo.com/hix/nm/20020122/wr/pope_internet_dc_1.html)

---

## ✶ Unshredders

"Peter G. Neumann" <[neumann@csl.sri.com](mailto:neumann@csl.sri.com)>

*Tue, 22 Jan 2002 9:27:13 PST*

The recent Enron/Anderson shredding frenzies suggest that it is time for UNSHREDDING software tools to come out of the closet. It is certainly feasible to restore a boxful of shreds, particularly for ordinary course-grain linear shredders. The effort for cross-cut shredders would be significantly more difficult, but still possible -- although probably less acceptable in court. Anything with some natural language or graphical context is likely to be recoverable, using digram, trigram, etc., statistics for the likely linguistic base(s) and other context. However, in general, it is probably easier to start out with backup tapes and incompletely deleted disks. Easiest of all would be to install scanners and transmitters (or local storage) in the shredder mechanisms, because that

would capture  
precisely the interesting materials deemed worth shredding.

There once was a swindler named Fred  
Whose enterprise went in the red.  
The lawmen he dreaded,  
So papers were shredded,  
And off to the races he fled.

---

## **⚡ Newspaper archives**

"Roger Needham" <needham@microsoft.com>

*Tue, 22 Jan 2002 07:52:55 -0800*

It is a principle in many jurisdictions that a jury should not know about prior charges or convictions of the accused. In a Scottish court a man was accused of a particularly revolting crime, he having been acquitted of a similar offence on a technicality a number of years ago. The judge ruled that the editor of a newspaper was in contempt of court by leaving reports of the earlier trial on line in his archive, because he had made it too easy for jurors to find out what they were not meant to know. The judge apparently believed that the greater ease of access of the on line archive as compared to a paper archive was a difference not of degree but of kind.

Roger Needham

---

## **✶ Virginia county recalls student laptops**

"NewsScan" <newsscan@newsscan.com>

*Mon, 21 Jan 2002 09:07:30 -0700*

Henrico County, Va. school officials are recalling all 11,000 laptop computers that it distributed to its high school students in order to retrofit them with security software that will prevent students from using the devices for accessing pornography or changing their grades -- abuses that reportedly have occurred since the machines were handed out last fall. Game and music downloading capabilities will also be eliminated or heavily restricted and instant messaging will be limited to home use. Teachers have complained that in-class use of entertainment file-sharing and messaging are disruptive. (AP/\*Wall Street Journal\*, 20 Jan 2002; NewsScan Daily, 21 Jan 2002) <http://interactive.wsj.com/articles/SB1011563803808773240.htm>

---

## **✶ Software uncovers e-mail untruths**

"NewsScan" <newsscan@newsscan.com>

*Mon, 21 Jan 2002 09:07:30 -0700*

SAS Institute has developed software that it says can sift through e-mails and other electronic text to discern falsehoods. "The patterns in people's language change when they are uncertain or lying," says Peter Dorrington,

business solutions manager at SAS. "We can compare basic patterns in words and grammatical structures versus benchmarks to detect likely lies." For instance, over-use of the word "or" and too many adjectives can be giveaways, according to Aldert Vrij's book, "Detecting Lies and Deceit." SAS says its software can also be used to detect inaccuracies in resumes and job applications. (\*Financial Times\*, 20 Jan 2002; NewsScan Daily, 21 Jan 2002) [news.ft.com/news/industries/internet&e-commerce](http://news.ft.com/news/industries/internet&e-commerce)

[Risks? What risks? PGN]

---

## **Georgia Tech anti-cheating software**

Walter Roberson <roberson@ibd.nrc.ca>  
*Sun, 20 Jan 2002 16:18:14 -0600 (CST)*

<http://fyi.cnn.com/2002/fyi/teachers.ednews/01/17/cheating.software.ap/index.html>

A recent CNN article describes a computer program that Georgia Tech has employed to detect cheating in its "Introduction to Computing" and "Object Oriented Programming" programming courses. 186 possible violations were found (over ~1700 enrolled students.)

I found this paragraph particularly interesting:

But for the most part, the degree of similarity that this program is looking for -- the commas are in the same place, the semicolons are in the

same place, the spacing is the same, they've made the same mistakes -- the

only explanation, and what most students will eventually concede, is they

actually did it," Eislet says.

It seems to me that placement of commas, semicolons and spacing would tend to be the same for the more experienced programmers who have adopted coding standards -- or for anyone who runs their program through a "code beautifier". (Unless perhaps Eislet was referring to the - comments- rather than the code!)

I gather from my readings and discussions with teachers of introductory programming classes, that, year after year, beginning programmers tend to make the same -kind- of mistakes. Gross syntactic mistakes are rejected by compilers, and modern compilers that would be used in teaching environments usually remark on error markers such as using assignment instead of comparison in an "if" statement; or use of a variable before it is initialized. This filtering that takes place in the compiler would tend to concentrate the errors more and more into common problem areas such as incorrect handling of boundary conditions, and failure to test return codes on I/O operations and library calls, so coding errors are -not- likely to be uniformly randomly distributed.

I would also note that every submitted program is being compared to every other submitted program for the same class, as "cheating" is pair-wise, not something that is in reference to an absolute standard. Anytime you have

pairwise interactions, the number of pairs goes up as the square of the number of samples. If the marker variables are discrete and are limited in range, then one encounters "the birthday paradox", wherein it takes an unexpectedly small number of samples in order to find -some- pairwise match. My calculation is that the probability of an accidental match would have to be less than 1 in 721292 in order for there to be less than a 50% chance that the program will deem at least two innocent students in a class of 1000 to have copied from each other.

Considering that Eislet is quoted as saying that for a match, "the only explanation" is that the students cheated, I would have to question whether the program authors undertook a proper statistical analysis.

---

## **✶ Anthrax mail irradiation can affect electronic devices in postal mail**

Thomas Dzubin <dzubint@vcn.bc.ca>  
*Tue, 8 Jan 2002 09:05:18 -0800 (PST)*

Story at: <http://uk.news.yahoo.com/020108/80/cnoy6.html>

"Compact flash memory cards used to store data on many name-brand digital cameras and handheld computers face not just data loss but become entirely inoperable when subjected to electron beam irradiation, the CompactFlash Association said on Tuesday"

(I just checked the CompactFlash Association web site at [www.compactflash.org](http://www.compactflash.org) and didn't see any related news-release about this, so I don't know how much research has gone into this assertion or if this is a potential birth of a new "urban legend")

It does bring up an interesting technology related risk

I think most (North-American) people make the following two assumptions:

1. postal service will generally deliver anything small & non-dangerous.
- and
2. postal service doesn't alter contents of things it delivers.

When you add "technology" to either of these in isolation, there is no problem. However the technology-related risk here is that when you add "technology" (irradiation & flash cards) to BOTH of these assumptions, the result can be unexpected and damaging.

Thomas Dzubin Network Analyst & PDP-11 enthusiast  
Vancouver, Saskatoon, or Calgary CANADA

---

## **✶ Health insurer computer changes delay payments...**

Don Mackie <[donald@iconz.co.nz](mailto:donald@iconz.co.nz)>  
*Sun, 20 Jan 02 11:19:06 +1300*

Southern Cross Healthcare, New Zealand's largest health insurer, bought out Aetna locally. At the time, acquisition of Aetna's patient and practitioner database was one of the Southern Cross's goals. Since before Christmas Southern Cross has run into increasing delays in paying claims. This has

caused cash flow difficulties for some private hospitals. Southern Cross published ads saying it was all due to difficulties with their new computer system. More recent articles tell us the predictable story - that the transition to a different system has, once again, been poorly handled.

<http://www.stuff.co.nz/inl/index/0,1008,1073278a11,FF.html>

<http://www.stuff.co.nz/inl/index/0,1008,1073362a1896,FF.html>

---

## ✶ Excel cut-and-pasting behaviour

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

*Fri, 18 Jan 2002 14:52:51 +1100*

Some time back, I was doing work that involved a lot of cut-and-pasting data between Excel files. Open source file, select cells, Ctrl-C, select destination file, Ctrl-V, repeat for dozens of source files.

I got tired of having lots of source files open at once, so I changed this slightly: open source file, select cells, Ctrl-C, close source file, select destination file, Ctrl-V, repeat.

At first this looked like it was accomplishing exactly the same thing, with exactly the same numbers appearing in the target cells, but when I tried further processing of the data (examining differences between adjacent cells) it became obvious that something was wrong - the results were much too 'grainy'.

Eventually I discovered the cause of the problem. When pasting from an open file, Excel correctly pastes the full contents of the selected cells. But if the source file is closed before pasting, it does not paste the full contents - only the *\*displayed\** contents. The result of this is to automatically round pasted data at the display precision (so with a precision of two decimal places, a value of 1.59835 would be pasted as 1.59835 from an open file, but as 1.60 if the file was closed before pasting.) And because the rounding precision here *\_is\_* the display precision, the pasted data looks correct until you change the precision to examine it...

Fortunately, the display precision I was using was low enough to make for very large errors, so it was obvious that there was a problem. At a slightly higher precision, I could quite easily have ended up with significant but non-obvious errors.

The risk here: one operation with two modes of behaviour that *\_look\_* identical, but aren't.

Geoffrey Brent

---

## **⚡ Lotus Notes silently losing data**

Erling Kristiansen <ekristia@xs4all.nl>

*Fri, 11 Jan 2002 21:19:14 +0100*

I have experienced several, apparently unrelated, incidents where Lotus Notes is quietly losing data.

\* I printed a mail message before I sent it. Some of the cc: addresses were quietly and permanently removed. (Did anybody say buffer overflow recently? Maybe it is more like buffer truncation, but certainly member of the same family)

\* Trying to reply to a mail I received, I discovered that 3 out of the about 10 cc: addresses in the incoming message had been truncated, rendering them invalid. No addresses were lost completely, but the amount of truncation that occurred suggests that a short address might be "truncated into extinction" if it is in the right place in the list of addresses. I checked the original RFC-822 header that is accessible. It was correct.

By the way, correcting the addresses in place and re-sending had a very strange effect: The corrected addresses, and only those, were turned into an X.400-like address with a number of attributes pointing to my local environment. I had to remove and re-type the "sick" addresses to have them accepted.

\* I copied and pasted about 100 addresses from a spreadsheet into the bcc: field of a mail. Everything looked OK, the pasted addresses appeared neatly in the address window, I could scroll through them, etc. But the message was only sent to the first address. No warning of any kind appeared that a

good hundred addresses had been discarded. I only discovered the error because I had asked for delivery notification, and got very few. Had I not discovered this, only a handful of people would have been invited to a presentation. (there were a few other addressees that had not been pasted in - those worked OK even though some were entered AFTER the skipped addresses).

\* Notes allows you to format messages, with facilities more or less equivalent to an HTML editor. If a message is sent outside the Notes domain, ALL formatting is removed, even things like indentation and paragraph numbers. So a nicely formatted message may become rather unreadable, even ambiguous (indentation may imply a lot about the meaning of a text). No warning is given that formatting information is being removed.

The RISK of all this is that Notes accepts instructions to do something, does not complain about the input, and then goes ahead and does something else than what could reasonably be expected. You can obviously check for any of these events, but they are rare enough, and different enough, that you don't really know when to expect a problem, and what to look for in order to make sure everything went as expected.

Erling Kristiansen

---

## **Woman says telephone makes unsolicited calls**

Carl Fink <carl@fink.to>

*Fri, 18 Jan 2002 13:17:49 -0500*

According to the *\*Detroit News\**, Becky Sivek doesn't even have long distance service. Nevertheless, "thousands" of long distance calls all over the USA are being made. The calls disconnect as soon as someone picks up. Some people are getting this same call dozens of times a day.

Although Sivek isn't making the calls, and they don't appear on her bill, caller ID shows her number, meaning that she's now getting many angry and/or threatening calls from people demanding she stop harassing them.

Phone phreaks, maybe?

<http://www.detnews.com/2002/metro/0201/18/d06d-393292.htm>

Carl Fink, I-Con's Science and Technology Programming <http://www.iconsf.org/>

---

## **✶ Answering machine provides door entry code**

Benjamin Elijah Griffin <eli@panix.com>

*Mon, 21 Jan 2002 14:32:33 -0500 (EST)*

On a recent Sunday, walking past an office building in my area a woman asked me for help getting into the building. She explained she had an appointment with a tenant in the building but couldn't get in. She had dialed the company's extension on an outside phone and gotten a recorded message to 'enter #2000 to come in, if you have an appointment'. The phone

used '##' to  
hang up calls, and it was the number of #s required that caused  
the problem  
for the woman, but I find it baffling that an answering machine  
is  
considered acceptable weekend security.

---

## ✂ Microsoft using predictable passwords for Passport?

Rodger Donaldson <rodgerd@diaspora.gen.nz>  
*Sun, 20 Jan 2002 09:03:01 +1300*

An organisation I am familiar with has a Microsoft support  
contract for the  
Microsoft components of their infrastructure; in order to access  
Microsoft's  
on-line resources, a Passport account is required. Microsoft  
has allocated  
the company a Passport account, with a numeric login whose  
password is set  
to the surname of their primary contact in the company.

The risk? This is a totally predictable scheme. It would be  
trivial to  
scan the numeric Passport logins looking for passwords set to  
common  
surnames.

Rodger Donaldson <rodgerd@diaspora.gen.nz>

---

## ✂ Re: Other blunders (La Fetra, [RISKS-21.86](#))

<brett@benders.net>  
*Thu, 10 Jan 2002 14:03:29 -0600*

In [RISKS-21.86](#), Skip La Fetra ('Other blunders on "secure" Web sites') claims that request parameters contained in a URL are not protected (encrypted) when the request is sent via a HTTPS GET.

This is a misunderstanding regarding the actual risk of using the GET method instead of the POST method. The traffic in an HTTPS session is always encrypted, whether the GET or POST method is used. However, use of the GET method encodes the parameters (including e.g. credit card numbers) into the request URL. This exposes such info in your browser history and in the site logs of the web server (rendering it vulnerable to the electronic equivalent of 'dumpster diving') -- the info is not, however, transmitted in cleartext.

---

## ✶ Re: Kaiser Permanente exposes medical record numbers

"George C. Kaplan" <gckaplan@ack.berkeley.edu>  
*Thu, 10 Jan 2002 13:48:35 -0800*

j debert <jdebert@garlic.com> writes in [RISKS 21.86](#)

> Kaiser Permanente has a Web site for members at <http://www.kponline.org/> .

>  
> The first page here is the signon page, where one enters a medical record number and their region to enter the site.

>  
> A statement concerning online security ... indicates in the first

> paragraph that the medical record number will be sent via SSL:  
> ...  
> However no SSL connection is possible. Every attempt to obtain  
a secure  
> connection gets redirected to the non-secure page.

It's not *\*quite\** this bad. True, if you try to go to  
<https://www.kponline.org>, you invariably get redirected back to  
the  
unprotected page. However, the ACTION part of the sign-on form  
points  
to <https://kponline.kp.org/signon/signonmember>, which is SSL-  
protected.  
All further interaction with the Kaiser site after signing on  
appears  
to be through SSL via [kponline.kp.org](https://kponline.kp.org).

But they make the same mistake mentioned by Skip La Fetra  
earlier in the  
same RISKS digest: the medical record number is transmitted in  
the URL. So  
Kaiser's claim is incorrect; the medical record number is not  
protected by  
SSL.

Once you've registered, you need a PIN to sign-on, and that *\*is\**  
sent via  
SSL, so the PIN and the rest of your session appear to be  
reasonably well  
protected. But in order to *\*get\** a PIN, the only  
"authentication" data  
required (besides the record number) is your full name.

I guess if you're a Kaiser member you should register on this  
site before  
someone else does it for you.

George C. Kaplan, Communication & Network Services  
University of California at Berkeley 1-510-643-0496  
[gckaplan@ack.berkeley.edu](mailto:gckaplan@ack.berkeley.edu)

## **✂ Re: Bogus dates for McAfee virus alerts (Colburn, [RISKS-21.85](#))**

David Blakey <djb@poboxes.com>

*Tue, 08 Jan 2002 11:33:43 +1300*

This is familiar to Web designers, and should be known by someone like McAfee.

First, many people have JavaScript turned off. If the script is not going to be completed, then the designer should have more sense than to write out the "This page current as of ". This should be included in the script as well, so that people with JavaScript turned off will not see anything at all.

Second, the JavaScript date may be presented by a source that is unreliable - such as the client's system date - or unsupported - such as "date modified" in some browsers.

The site seems to lack a good "sniffer" to find out (1) if JavaScript is on and (2) if the "date modified" function is supported. There is little risk presented by this site, but one wonders if the people who designed it have since moved on to emergency services or air traffic or defence sites.

---

## **✂ Re: AOL's spam filters (Burstein, [RISKS-21.85](#))**

"Jay Levitt" <jay@jay.fm>

*Sat, 19 Jan 2002 21:59:26 -0500*

> Also note that a "bounce" message would take this whole saga out of the  
> "risks" venue (or at least move it to the margin).

Would that that were true, but bouncing spam merely introduces new risks.

I was intimately involved in AOL's mail system for most of the past decade, and our motto was It's Not That Simple.

AOL hasn't always had spam filters. Years ago, we would see huge numbers of bounce messages generated for spam runs, since spammers often send to e-mail addresses that are no longer valid. One spammer actually sued us for delivering his bounces back to him - he said we were trying to overload his small mail server! (Apparently the huge volume crashed it.) And once spammers started forging return addresses, these bounces began causing no end of trouble for the poor site that found itself receiving millions of undeliverable e-mail reports from AOL. Additionally, we had to make sure that these huge queues of bounce e-mails didn't interfere with the delivery of legitimate communications, or even bounces of legitimate communications. Far from taking minutes to deliver, these bounce queues can quickly back up to infinity without constant babysitting.

With SMTP, if you can detect that a message is undeliverable early enough in the process, you can simply refuse it, rather than bounce it back. But that presumes that the machine sending to you is the originator of the message. Spammers often relay their e-mail off unsuspecting third-party mail servers that are configured to accept mail from anywhere

and deliver  
it to anywhere. (This was the default configuration of all mail  
servers  
until just a few years ago; remember, the Internet began as a  
cooperative  
effort.) If you refuse mail from a third-party relay, THEY then  
have to  
deliver the bounce messages, which again can crash or hobble  
their systems.

Of course, if you simply turn off spam filters on a system as  
target-rich  
as AOL, you're left with a fairly useless mail system - we've  
often  
estimated that 30-50% of all the incoming messages are spam.

I've since left AOL, but I know that the folks there were doing  
everything  
they could to detect spam as early in the transaction as  
possible, and  
refusing it rather than bouncing it whenever they could.

The real risk is taking a protocol designed to cooperatively  
exchange  
messages within a small community, and using it for worldwide,  
mission-  
critical communications, sometimes from hostile senders. The  
rest is  
imperfect band-aids.

---

## **✶ Call for Participation Open Source Software Development Workshop**

Cliff Jones <cliff.jones@ncl.ac.uk>  
*Sun, 20 Jan 2002 17:29:17 +0000*

WORKSHOP ON OPEN SOURCE SOFTWARE DEVELOPMENT, 25-26 FEBRUARY 2002  
Newcastle upon Tyne, UK

<http://www.dirc.org.uk/events/ossdw/main.html>

The focus of the Open Source Software Development workshop is on dependability and open-source software development.

Dependability is a deliberately broad term which, among others, covers reliability, security, safety and availability.

We have put together an exciting programme and would welcome further participation from the community. Participation would be particularly welcomed from any of those engaged in, or affected by, the design, development or operation of open source software. An important objective of this workshop is a greatly improved understanding of the complete organisational and cultural context of complex systems of which computers are a part. To this end, we especially encourage participation from interdisciplinary researchers and practitioners, since we believe that such research is crucial for progress towards the safe deployment of new technologies.

Those interested in participating in this event should send an e-mail stating their interest to [Cristina.Gacek@ncl.ac.uk](mailto:Cristina.Gacek@ncl.ac.uk), preferably by 15th February 2002.

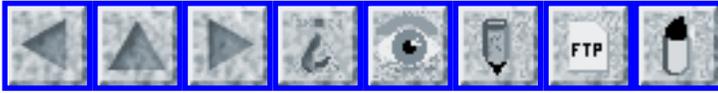
Cristina Gacek, Centre for Software Reliability (Bedson Building)

Department of Computing Science, University of Newcastle upon Tyne

NE1 7RU - United Kingdom Telephone: (44 191) 222 5153

FAX: (44 191) 222 8788 [cristina.gacek@ncl.ac.uk](mailto:cristina.gacek@ncl.ac.uk)

---



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 21: Issue 89**

**Tuesday 29 January 2002**

## Contents

- [Wireless technology criticized for vulnerabilities](#)  
[NewsScan](#)
- [Wireless bypassing the firewall](#)  
[Jeremy Epstein](#)
- [Free airport wireless network, and spam launcher](#)  
[Mike Hogsett](#)
- [Consumer beware: Are you really there?](#)  
[Rob Graham](#)
- [Risks of deceptive characters in URLs: Gabrilovich/Gontmakher](#)  
[PGN](#)
- [Water line break closes 911 center & police department](#)  
[Dave Bank](#)
- [New official self-service litigation system available in England & Wales](#)  
[Tony Ford](#)
- [Royal chat session failed](#)  
[Erling Kristiansen](#)
- [Risks of bouncing e-mail](#)  
[Nick Brown](#)
- [Stupid defaults in database conversion](#)  
[Paul Wallich](#)

- [Spam prevention gone too far](#)  
[Jonathan Kamens](#)
  - [BBC News: Iceland places trust in face-scanning](#)  
[Chris Leeson](#)
  - [Brisbane ISP in court](#)  
[Peter Deighan](#)
  - [RSA Conference e-mail has tracking bugs](#)  
[Rex Sanders](#)
  - [Re: Buffer overflows and other stupidities](#)  
[Earl Boebert](#)
  - [Re: Software uncovers e-mail untruths](#)  
[Russ Perry Jr](#)
  - [Remote mobile phone configuration changes via SMS service](#)  
[S. Llabres](#)
  - [REVIEW: "Algebraic Aspects of Cryptography", Neal Koblitz](#)  
[Rob Slade](#)
  - [Infowar Con 2002, call for papers](#)  
[Winn Schwartau](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

## ⚡ **Wireless technology criticized for vulnerabilities**

"NewsScan" <newsscan@newsscan.com>

*Tue, 29 Jan 2002 08:37:15 -0700*

Lawrence Livermore National Laboratory in California has banned all wireless networks, including Microsoft's Wi-Fi, because of security concerns. Wi-Fi supporters say the technology is secure when it's been properly installed, but experts say that only about 10% of all users install them correctly.

(\*USA Today\*, 28 Jan 2002; NewsScan Daily, 29 January 2002)

<http://www.usatoday.com/life/cyber/tech/2002/01/29/wifi.htm>

## **⚡ Wireless bypassing the firewall**

"Jeremy Epstein" <jepstein@webmethods.com>

*Fri, 25 Jan 2002 17:01:13 -0500*

Wireless carriers including Sprint, Cingular, and Seven (a startup) are putting together products that tunnel through the firewall to allow you to access the e-mail, calendars, etc. on your desktop machine remotely from a wireless device. But not to worry, since it "conforms to the highest levels of transport security". After all, what could go wrong with a tunnel like this? NOT! The risks are apparent to everyone except the vendors involved.

Full story at

<http://www.infoworld.com/articles/hn/xml/02/01/28/020128hnport.xml>

---

## **⚡ Free airport wireless network, and spam launcher**

Mike Hogsett <hogsett@csl.sri.com>

*Tue, 29 Jan 2002 13:13:03 -0800*

Soon business travelers passing through Minneapolis-St. Paul International Airport will be able to access the Internet at high speeds for free.

Anyone want to send out lots of SPAM or launch attacks? Just go to MSP.

<http://www.startribune.com/stories/535/1130636.html>

---

## **⚡ Consumer beware: Are you really there?**

"Rob Graham" <ceo@grahamsolutions.com>

*Mon, 28 Jan 2002 10:46:57 -0500*

This potential risk was sent to me at work today. At a quick glance of the site below, you may truly feel that you've made a drastic mistake at microsoft.com, or the evil doings of a disgruntled employee. I as a Web developer and consultant quickly determined how it was done (simply passing a username and password to the true url to display the page). However, a link contained within an e-mail to the unsuspecting consumer bringing them to a site like this could be a disaster.

This false representation is an easy way to exploit information from a consumer thinking they are buying/subscribing/requesting information from a company - when in fact, it may be a scenario like the link below:

[www.microsoft.com&item=3Dq209354@hardware.no/nyheter/feb01/Q209354\\_%20-%20HOWTO.htm](http://www.microsoft.com&item=3Dq209354@hardware.no/nyheter/feb01/Q209354_%20-%20HOWTO.htm)

---

## **⚡ Risks of deceptive characters in URLs: Gabrilovich/Gontmakher**

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

Mon, 28 Jan 2002 22:45:21 PST

Related to Rob Graham's item in [RISKS-21.89](#), an even more insidious URL risk is described in an excellent column on the Inside Risks page of the February 2002 CACM:

Evgeniy Gabrilovich and Alex Gontmakher

The Homograph Attack

Communications of the CACM, vol 45, no 2, inside back page

This is a WONDERFUL RISKS-relevant article. Please read it. For your convenience, this column is now on the Inside Risks Web site

<http://www.csl.sri.com/neumann/insiderisks.html>

as

<http://www.csl.sri.com/neumann/insiderisks.html#140>

The examples given use Cyrillic characters. For example, a Russian "o" and an English "o" look alike but can have radically different results.

---

## **Water line break closes 911 center & police department**

Dirk the Daring <dirk@psicorps.org>

Thu, 24 Jan 2002 17:19:08 -0500 (EST)

<http://www.newsobserver.com/ncwire/news/Story/903276p-902507c.html>

In Durham, NC (USA), a waterpipe break on early Saturday (12-Jan-2002) morning forced the closure of the city police department building and 911 center. The water flooded a subbasement and took out the

electrical  
equipment and backup power generators. Callers to 911 got busy  
signals or  
disconnects (I suppose that's better than hold muzak) until the  
temporary  
location (at Duke University) was online about 12 hours later,  
with  
dispatchers taking call information on paper (no computers).

RISKS:

1) Putting all the eggs, police dept and 911 center, in one  
building

2) Putting critical electrical equipment in a place where it  
can  
be easily flooded out and in the same building

3) Not having 911 services "roll-over" to somewhere else  
(for example,  
Cary, NC - about 20 miles from Durham - has an agreement  
with  
the Wake County 911 center that if Cary becomes unable  
to take a  
given 911 call, it automatically rolls over to Wake's 911  
center) - a (\*gasp\*) backup

Dave Bank aka Dirk the Daring dirk at psicorps dot org

---

## **⚡ New official self-service litigation system available in England & Wales**

Tony Ford <tony.ford@net.ntl.com>  
*Sat, 26 Jan 2002 15:43:09 +0000*

Today's Daily Telegraph (a quality UK broadsheet newspaper)  
carries a  
\*potentially\* disturbing report describing a new service, "Money

## Claim

Online", whereby individuals and law firms (solicitors) can issue most simple legal proceedings (where a sum less than UK pounds 100,000 is claimed, = USD 140K)) and enforce judgments via a Web browser. The new service has been set up without publicity by the Lord Chancellor's Department, which runs the courts system in England and Wales. It seems that the system is accessible to the public now, although it has not been officially launched.

People using the service are (oddly) referred to as "customers" .... and there is a Customer Help Desk ...

The newspaper report is also viewable at this Daily Telegraph link on-line:

[www.telegraph.co.uk/news/main.jhtml?xml=/news/2002/01/26/nsue26.xml&sSheet=/news/2002/01/26/ixhome.html](http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2002/01/26/nsue26.xml&sSheet=/news/2002/01/26/ixhome.html)

The service can be seen on-line at:

<https://www.moneyclaim.gov.uk/csmco/index.html>

No details are apparent of what measures are taken to validate the identity of the claiming party or prevent other gross miscarriages of justice ....

but it would appear that the potential exists for significant trouble ....

even though the site warns that "vexatious litigants" are not allowed to us

it (these are people who have abused the litigation system in the past to

such an extent that they have been declared "vexatious litigants",

restricting their ability freely to issue legal proceedings).

PS: I am a lawyer myself, although I don't practise in this area .. but do

work in-house for a large IT company ... these comments are offered purely in a personal capacity.

Tony Ford, Guildford, Surrey, UK <tony.ford@net.ntl.com>

---

## ✶ Royal chat session failed

Erling Kristiansen <ekristia@xs4all.nl>

*Wed, 23 Jan 2002 21:20:45 +0100*

A public chat session was scheduled yesterday between, on one hand, the Dutch Crown Prince Willem Alexander and his fiancée Maxima Zorreguieta and, on the other hand 100 selected citizens. The session was made available for everybody to watch on a Web site.

The server failed after a few minutes and did not come up again, so the rest of the session was canceled.

According to several news sources (radio and TV news, printed press), KPN, who provided the server, says that the crash was caused by "sabotage", and that the site, that was designed for "tens of thousands" of users, received 3 billion (Yes, 3,000,000,000) hits.

The story does not look very plausible to me. To deliver 3,000,000,000 IP packets, even short ones, in a few minutes takes something like a 10 Gbits/sec connection into the server, and would require quite a powerful attacking machine with a comparable network connection, or a concerted

attack by tens of thousands of home PC's on modem lines.

I also had a look at

<http://internettrafficreport.com>

Such a volume of traffic in a short time should cause some slowdown of other

Internet traffic in the networks concerned. I saw no noticeable performance

degradation in any of the Dutch routers monitored by this site, nor anywhere

else, around the time of the event.

Speculation in the media now goes that the site simply received more genuine

hits than it was designed for, but not billions (Holland has 16 million

inhabitants), and could not cope, and that KPN is reluctant to admit their

mis-estimation of the traffic.

Does anybody have more information about what really happened?

---

## **⚡ Risks of bouncing e-mail**

BROWN Nick <Nick.BROWN@coe.int>

*Thu, 24 Jan 2002 08:50:21 +0100*

The Strasbourg newspaper "Dernières Nouvelles d'Alsace" reports (in French)

an interesting case of e-mail forgery. The exact circumstances are not yet

clear, but it appears that:

- An e-mail was sent from the account of the mayor, telling members of a

city commission to vote in favour of a plan to extend a local hypermarket.

The official, public policy of the city council and the mayor is

to oppose

this extension.

- The mail to one member of the commission bounced, because the recipient's

name was incorrectly spelled.

- An assistant to mayor Fabienne Keller, who has access to her mailbox,

noticed the "undeliverable" reply and determined that the mail had been sent

at a time when the mayor could not have sent it.

- The general manager of the hypermarket is under police investigation for

illegal entry into a computer system, forgery, use of forged documents, and

attempted fraud.

Original texts in French for those interested:

> [www.dna.fr/cgi/dna/motk/idxlist\\_light?](http://www.dna.fr/cgi/dna/motk/idxlist_light?a=art&aaaammjj=200201&num=180)

[a=art&aaaammjj=200201&num=180](http://www.dna.fr/cgi/dna/motk/idxlist_light?a=art&aaaammjj=200201&num=180)

> [41610&m1=keller&m2=mairie&m3=](http://www.dna.fr/cgi/dna/motk/idxlist_light?a=art&aaaammjj=200201&num=19049910&m1=keller&m2=mairie&m3=)

[www.dna.fr/cgi/dna/motk/idxlist\\_light?](http://www.dna.fr/cgi/dna/motk/idxlist_light?a=art&aaaammjj=200201&num=19049910&m1=keller&m2=mairie&m3=)

[a=art&aaaammjj=200201&num=19049](http://www.dna.fr/cgi/dna/motk/idxlist_light?a=art&aaaammjj=200201&num=19049910&m1=keller&m2=mairie&m3=)

[910&m1=keller&m2=mairie&m3=](http://www.dna.fr/cgi/dna/motk/idxlist_light?a=art&aaaammjj=200201&num=19049910&m1=keller&m2=mairie&m3=)

I suppose the RISK is that if you're going to pretend to be someone else,

make sure you can spell !

Nick Brown, Strasbourg, France

---

## ✶ Stupid defaults in database conversion

Paul Wallich <pw@panix.com>

*Fri, 25 Jan 2002 17:20:05 -0500*

Even in the sticks there are risks:

Last autumn, the propane company that fills our tank (for stove, hot water and drier) was taken over by another propane company. We learned last night, when all of our gas-fired appliances stopped working, that "some customers fell through the cracks" during the acquisition, to wit, the new company wasn't refilling their tanks and was apparently relying on calls like ours to let it know whom it had forgotten. They promised a delivery "first thing" in the morning. So about noon we called, and learned a few additional tidbits: apparently customers scheduled for regular deliveries from the old company had been silently changed to "will call" status by the new one, and no, the new company didn't believe it had any liability for interrupted service.

The risk of mistranslating fields in an acquired database should be obvious, as should the rule that any untranslatable values get flagged and/or at least converted to the least-damaging equivalent in the new system. (There's also the obvious financial risk that customers won't want a company that careless involved in delivering a commodity know to blow folks to bits when mishandled.)

---

## **✶ Spam prevention gone too far**

Jonathan Kamens <jik@kamens.brookline.ma.us>

*Thu, 24 Jan 2002 16:23:17 -0500*

I recently attempted to send E-mail to the author of a RISKS submission. Since my DSL line was down when I sent the E-mail, and since outbound SMTP connections are blocked from the dial-up accounts provided by my ISP, I had to send my E-mail through my ISP's mail server. It bounced as follows (the identify of the intended recipient has been masked):

<RECIPIENT@RECIPIENT-HOST>:

Connected to RECIPIENT-HOST-IP but sender was rejected.

Remote host said: 571 <jik@kamens.brookline.ma.us>... Return address jik@kamens.brookline.ma.us does not match sending computer mail11.speakeasy.net -- check your configuration. [http://www.RECIPIENT-HOST/mail/571\\_2.html](http://www.RECIPIENT-HOST/mail/571_2.html) for details.

If you visit the URL referenced above, you discover that this site's system administrators have decided to block all E-mail for which the host name in the envelope address can't be matched up obviously (using a simple string comparison) with the host name of the mail server sending the message. In other words, if you have your own domain name, but you send E-mail through your ISP's mail server, you simply can't send E-mail to this site. Supposedly, they check their logs for such bounces "as we have time" and add messages that should have gone through to an exception list, but who knows when/if they'll ever get around to doing that in any particular case. Furthermore, they provide no mechanism for contacting them by E-mail or Web to ask to be excepted -- all they give on the Web page is a long-distance telephone number.

Fortunately for me, or so I thought, I \*do\* send outbound mail through my

own mail server when my DSL line is up, and it was fixed yesterday, so I decided to attempt to resend my message. It bounced again, with a different error:

RECIPIENT@RECIPIENT-HOST

(reason: 550 We do not accept mail from the spam-relay machine: jik-0.dsl.speakeasy.net.. [http://www.RECIPIENT-HOST/mail/571\\_1.html](http://www.RECIPIENT-HOST/mail/571_1.html) for details.)

If you visit *that* URL, you see that they're claiming that my machine is a spam relayer. It isn't and never has been. I've never sent spam and I block all third-party relaying through my machine. I can't find an entry for either my IP address or my subnet in any of the black-lists checked by

<URL:<http://relays2.osirusoft.com/cgi-bin/rbcheck.cgi>>.

Of course, they don't bother to say *why* they think my machine is a spam-relay machine, so who knows where they got that charming idea? And, as mentioned above, they don't provide any way to contact them on-line to complain about it. For example, many sites which enforce restrictions this draconian provide an address which is exempt from the restrictions to which people can complain; the spammers don't ever bother complaining, so it really isn't particularly burdensome to do this. Unless, of course, you really don't care if people can't send legitimate E-mail to your site.

I understand the desire to block spam, but there are ways to do it which don't also block legitimate E-mail, or at the very least which provide an on-line mechanism people can use for getting themselves

unblocked. This is just really excessive; I would even go so far as to say that I question the legitimacy of allowing RISKS submissions from people who make it impossible for people to send them E-mail responses to their submissions.

jik

---

## **✶ BBC News: Iceland places trust in face-scanning**

"LEESON, Chris" <CHRIS.LEESON@london.sema.slb.com>

*Fri, 25 Jan 2002 09:40:31 -0000*

According to the BBC News Web Site, Iceland's main airport is introducing "face recognition technology" to identify "any hijackers on wanted lists".

[http://news.bbc.co.uk/hi/english/sci/tech/newsid\\_1780000/1780150.stm](http://news.bbc.co.uk/hi/english/sci/tech/newsid_1780000/1780150.stm)

The article notes that a similar system was tried in Florida, and abandoned after two months. The article notes:

" 'In my opinion, had this system been installed at airports in North

America last summer, it would have increased the chances of catching those

criminals who hijacked the planes,' said Keflavik airport police

commissioner, Johann Benediktsson. [...] A recent report by the America

Civil Liberties Union showed that over a two-month period, the software

failed to identify a single person photographed in the department's

criminal database. Instead, the software produced many false identifications, said the ACLU report. [...]

"For Jonina Bjartmortz, a member of the foreign affairs committee in the

Icelandic parliament, the system has become a sure way of reassuring

nervous passengers. 'We are at the western most tip of Europe and a

gateway to America. We only have one airline and we felt it was very

necessary to invest in the technology,' she said. It seems to have

worked. Flights coming and going from Keflavik airport are generally full

and passengers appear happy."

One is tempted to say "The Usual Risks":

- False Positives and False Negatives
- Customers (and Management) with a potentially false sense of security
- It will only pick up "known" faces. What if your hijacker not "known"?

That said, we can hope that the existing security precautions will pick up

the "unknown" hijackers. At least the risk is no greater unless security

staff come to rely on the system.

Chris Leeson

---

## **✶ Brisbane ISP in court**

Peter Deighan <deighanp@ozemail.com.au>

*Thu, 24 Jan 2002 21:17:40 +1100*

The following is the entirety of a story printed in \*Australian Financial

Review\* 21 Jan 2002, attributed to Australian Associated Press:

"Dateline in court"

"The ACCC has begun legal action against Brisbane-based Internet provider Dataline.net.au, its managing director, Mr John Russell, and

associated companies Australis Internet and World Publishing Systems.

Dataline allegedly intercepted e-mails and debited consumers' credit cards without authority."

ACCC stands for Australian Competition and Consumer Commission, or in tabloid-ese "The consumer watchdog".

Other contributors to RISKS have mentioned packet sniffing and electronic

"dumpster diving" to extract credit-card numbers. This looks to be much

simpler. If the ACCC is correct, this seems a good reason to become an ISP.

Is this a new risk? Probably not.

The full and more worrying set of allegations is at ACCC's Web site:

<http://www.accc.gov.au/media/mediar.htm>

then click on

18 January 2002 ACCC Takes Action Against Internet Service Provider

Peter Deighan <deighanp@ozemail.com.au>

---

## **✶ RSA Conference e-mail has tracking bugs**

Rex Sanders <rsanders@usgs.gov>

*Thu, 24 Jan 2002 17:10:14 -0800*

Today I received the "RSA Conference 2002 eNewsletter, Volume 2". Much to my dismay, this HTML-ized e-mail had several hidden tracking features, including the classic 1x1 pixel GIF with a unique identifier encoded in the URL pointing to a company I've never heard of.

RISK: assuming you can trust e-mail from a conference and a company (RSA Security, Inc. sponsors the conference) which emphasizes security and privacy.

-- Rex Sanders, USGS

---

## ✶ **Re: Buffer overflows and other stupidities ([RISKS-21.87](#))**

Earl Boebert <boebert@swcp.com>  
*Wed, 23 Jan 2002 07:56:09 -0700*

[Earl Boebert's message in [RISKS-21.87](#) provoked many responses that are not included in this issue of RISKS, but to which Earl offered the following generic response. PGN]

Well, I'm glad I provoked at least some discussion of the issue. Unfortunately, many of the responses, including some from people who should have known better, exhibited a depressing degree of ignorance about the role of processor architecture in implementing protection mechanisms. To respond to these in detail would involve the moral equivalent of a course in the subject, which I do not currently have either the time or the inclination to

do. I would refer interested parties to Dick Kain's book [1], which (along with some of the more informative replies) shows that there are more things in heaven and earth than dreamt of in the x86 philosophies. I suppose a final note would be: Relying on any one element of an integrated hardware-software system for protection from hostile code is dangerous. Currently popular processor architectures contain such stupidities that they place an impossible burden on software and programmer discipline. Yes, these things can shoulder the burden in theory, but the historical evidence is that they fail consistently in practice.

[1] If you don't know this reference, you probably shouldn't be in this business.

---

## **⚡ Re: Software uncovers e-mail untruths (NewsScan, [RISKS-21.88](#))**

Russ Perry Jr <slapdash@enteract.com>

*Tue, 22 Jan 2002 22:24:14 -0600*

> SAS Institute has developed software that it says can sift through

> e-mails and other electronic text to discern falsehoods.

It would be interesting to take a press release or privacy statement

regarding this product and run them THROUGH said product, ne?

Russ Perry Jr      2175 S Tonne Dr #114      Arlington Hts IL 60005  
847-952-9729      slapdash@enteract.com

## **Remote mobile phone configuration changes via SMS service**

Llabres <sllabres@baden-online.de>

*Fri, 25 Jan 2002 01:40:36 +0100*

The German publishing house "Heise" reports in its online news about a remote configuration change of mobile phones via the short message service

(SMS) which is available in GSM networks:

<http://www.heise.de/newsticker/data/pmz-24.01.02-000/>

The Swiss telco Swisscom has confirmed that it has sent to selected customers special SMS messages that deleted roaming information on the SIM cards of the customers' mobile phones. Swisscom says that the purpose for the messages is to test for the introduction of new services in the Swisscom mobile phone network. The customers have not been informed about the change. The SMS appeared as empty messages sent from the phone number "0800".

The magazine also reported that insiders believe that the modification of the roaming information was to direct traffic to networks owned by Vodafone -- which acquired a 25% share of Swisscom on april last year.

Customers have to re-enter the information to their phones manually.

It would be interesting:

- \* If there is any security mechanism protecting anyone from sending such "special" messages.
- \* Which setting on the mobile phone can be changed (or probably retrieved from the phone) without knowledge to the customer.

\* If the network provider must implement such features, I do not understand why this must happen unperceived by the customer. Why not send a message telling people what will happen?

S.Llabres

---

## ✈ **REVIEW: "Algebraic Aspects of Cryptography", Neal Koblitz**

Rob Slade <rslade@sprint.ca>

Mon, 28 Jan 2002 07:37:01 -0800

BKALASCR.RVW 20011122

"Algebraic Aspects of Cryptography", Neal Koblitz, 2001,  
3-540-63446-0, U\$64.99

%A Neal Koblitz koblitz@math.washington.edu

%C 175 Fifth Ave., New York, NY 10010

%D 1998

%G 3-540-63446-0

%I Springer-Verlag

%O U\$64.95 212-460-1500 800-777-4643

%P 206 p.

%T "Algebraic Aspects of Cryptography"

When certain technical people find out that I am involved in data security, they assert an interest in cryptography, and an intention to write a cryptographic program sometime. While I not wish to disparage this goal, questioning of the individual's background in mathematics tends to point out that the task is harder than they might have foreseen. The magic phrase "number theory" is usually the dividing line. For those who make it past that limit, I am going to recommend that they get Koblitz's work. Not that I am implying that this book is more demanding than it needs to

be: only  
that the topic itself is a difficult one.

This is the heart of cryptology: the underlying foundations that make it work. The material presented does not address specific programs, standards, or even algorithms, but deals with the basic mathematical theory that can be used to construct algorithms, or test their strength.

Chapter one is something of an overview, touching on many fields of cryptography and introducing an appropriate and exemplar equation for each. Theories related to the strength of cryptographic algorithms are given in chapter two. Basic algebra associated with primes are discussed in chapter three, underlying the more common asymmetric (public key) systems such as RSA. Chapter four outlines an illustrative history of the development, cracking, and improvement of one particular algorithm, demonstrating the mathematical work necessary to each step. Knapsack type problems and theories are explained in chapter five. Chapter six deals with the currently very highly regarded elliptic curve algorithms, and is backed up with an even more extensive appendix on hyper-elliptic curves.

This is not an introduction. It is intended as a text for graduate (or possibly advanced undergraduate) work, and requires a solid background in mathematics or engineering. For those seriously interested in cryptography, though, it is worth the work.

copyright Robert M. Slade, 2001    BKALASCR.RVW    20011122  
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/>

---

## ✶ Infowar Con 2002, call for papers

Winn Schwartau <winns@gte.net>

*Wed, 23 Jan 2002 09:24:27 -0500*

Homeland Defense & CyberTerrorism:

Dealing With Harsh New Realities

3-6 Sep 2002, Washington, DC

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

Your Sponsors:

Winn Schwartau, Interpact, Inc. - [www.interpactinc.com](http://www.interpactinc.com)

MIS Training Institute - [www.misti.com](http://www.misti.com)

White Wolf Consulting [www.whitewolfconsulting.com](http://www.whitewolfconsulting.com)

We are soliciting creative analytic, interoperable real-world opinions and

solutions that will function in:

- \* Countering the threats of Global and National Cyberterrorism
- \* National and Municipal Critical Infrastructure Protection
- \* Military and Government Information Operations (Defense and Offense)

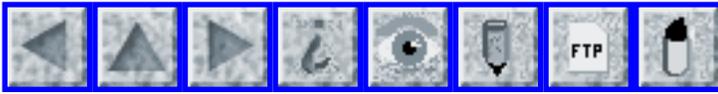
Submission Deadline: February March 11, 2002 [sic. one or the other? PGN]

For inquiry or discussion on submissions, please contact Winn Schwartau at

1-727-393-6600, or [InfowarCon@Earthlink.Com](mailto:InfowarCon@Earthlink.Com) or [winns@gte.net](mailto:winns@gte.net).

Winn Schwartau, President, Interpact, Inc. [www.security-aware.com](http://www.security-aware.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 21: Issue 90

**Sunday 10 February 2002**

## Contents

- [Software bug blamed in radioactive spill](#)  
[Adam Shostack](#)
- [CT unemployment insurance folk mail out "off by one" letters](#)  
[Danny Burstein](#)
- [Adult content filter considers MSDN Flash as "Unwanted adult spam"](#)  
[G.J. Dekker](#)
- [HP annual report bitten by spelling software](#)  
[Jim Griffith](#)
- [Turning Macs on Thievery](#)  
[Monty Solomon](#)
- [Instructive story](#)  
[Edward W. Felten](#)
- [E-commerce website automatic response proves costly](#)  
[Brian Ally](#)
- [Automated upgrade means no statistics](#)  
[Paul Roberts](#)
- [Yet another Microsoft Outlook exploit](#)  
[Bear Giles](#)
- [Bug in MS Excel?](#)  
[Alberto](#)

- [Re: Excel cut-and-pasting behaviour](#)  
[Peter Jeremy](#)
  - [UK to try remote voting](#)  
[Merlyn Kline](#)
  - [Miami-Dade OKs touchscreen voting](#)  
[David E. Price](#)
  - [Re: Even unscientific elections get rigged](#)  
[Joe Thompson](#)
  - [Re: Woman says telephone makes unsolicited calls](#)  
[William Kucharski](#)
  - [More Kaiser followup](#)  
[Geoff Kuenning](#)
  - [Re: REVIEW: "CISSP Examination Textbooks", S. Rao Vallabhaneni](#)  
[Rob Slade](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

## ✂ Software bug blamed in radioactive spill

Adam Shostack <adam@zeroknowledge.com>

Wed, 30 Jan 2002 13:45:14 -0500

<http://news.com.com/2100-1001-826124.html>

Andrew Colley, CNET News.com, 30 Jan 2002

SYDNEY, Australia--Amec Engineering, which designed the Beverly uranium processing plant in Western Australia, has blamed buggy software for a radioactive spill that occurred at the site last December, confirming early suspicions that computers played a role in the accident. "After a detailed assessment of the incident it is now clear that the problem was caused by a computer programming error that has since been corrected," said Stephen Middleton, spokesman for the plant's operator, Heathgate

Resources.

According to Amec's report, the glitch cut power to the plant's fluid-distribution control system during a routine service exercise. At the time, the mechanism should have shut down pumps moving fluid into the plant.

"Before they could be shut down manually, pressure built up in the pipelines leading into the plant and one ruptured," Middleton said.

According to Middleton, Amec has re-examined the entire system, retested the plant's pipes and corrected the "computer logic error." He refused to name the software technology responsible for the error.

[It doesn't sound to me like a software error that pipelines had no pressure gauges or relief valves; but it's always hard to say how correct media reports are. Does Australia have freedom of information laws or other means of access to see Amec's report? Adam]

---

## **CT unemployment insurance folk mail out "off by one" letters**

danny burstein <dannyb@panix.com>

*Fri, 25 Jan 2002 23:32:54 -0500 (EST)*

Labor Department finds error in unemployment compensation tax forms

An error has been found on tax forms sent to Connecticut residents who

collected unemployment compensation last year, the state Department of

Labor announced Friday. About 5,000 forms -- less than 3 percent of the

176,000 tax forms sent -- contain information pertinent to

individuals

other than the named unemployment compensation recipient.

[...] [Source

unspecified, 25 Jan 2002]

The article doesn't go into much more detail, but it sounds like a classic

mix and merge problem, with the headers for the mailing labels being off by

one (or more...) from the other data fields.

Nothing on the CT Web site about this yet.

---

## **✂ Adult content filter considers MSDN Flash as "Unwanted adult spam"**

"Dekker, G.J." <gjdekker@nlr.nl>

Wed, 23 Jan 2002 08:27:40 +0100

The Microsoft e-mail newsletter MSDN Flash, Volume 6, Number 2, January 22,

2002, contains advertising text including the text (Copied almost literally;

note: I added one extra space after the word "over" to circumvent the Microsoft filters.)

> Plus, VSLive! San Francisco provides over 180 hours of  
> content in three technical conferences:

The standard Microsoft "Adult Content Filter" includes the rule that a

message body containing the text "over 18" is Adult Content.

[SPACE

added by PGN in hopes of avoiding filtering?]

As result, the MSDN Flash was rejected by Outlook, as being unwanted adult

content.

I Wonder how many Microsoft customers have read this number of the Flash.

Geert Jan Dekker, National Aerospace Laboratory (NLR),  
P.O. Box 153,8300 AD Emmeloord The Netherlands +31 527 248435

---

## ⚡ HP annual report bitten by spelling software

<griffith@olagrande.net>

*Tue, 29 Jan 2002 19:42:45 -0600 (CST)*

An oldie but a goodie. AP reports that HP's annual report filed Tuesday mentions the names "David and Lucite Packard Foundation", "Edwin van Pronghorns", "Eleanor Hewlett Limon", and "Mary Hewlett Gaffe", instead of "Lucile", "Bronkhorst", "Gimon", and "Jaffe", respectively.

<http://www.siliconvalley.com/docs/news/tech/085146.htm>

---

## ⚡ Turning Macs on Thievery

Monty Solomon <monty@roscom.com>

*Sun, 27 Jan 2002 20:39:46 -0500*

In a story that is probably unique, R.D. Bridges recovered his sister's stolen iMac using Netopia's Timbuktu Pro, a program that allows computers to be remotely controlled and is widely used by computer-help technicians.

Bridges, who lives in Clear Lake, a suburb of Houston, had installed the software to help his sister, who lives across town, when she ran into problems. [...]

<http://www.wired.com/news/mac/0,2125,50025,00.html>

Tracing a Stolen iMac Using Timbuktu

<http://www.macscripter.net/unscripted.html>

---

## **🔥 Instructive story**

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

*Mon, 04 Feb 2002 15:54:30 -0800*

Here is a true story that illustrates several familiar RISKS.

My sister-in-law Karen Rakow was quite surprised recently to discover that according to a web site called slatkinfraud.com, she and her husband Robert had pocketed more than \$5 million from a Ponzi scheme in which they were involved. All of this was false -- including the part about having a husband named Robert. The accusation on the web site hyperlinked to Karen's business and to her list of clients, and it even named one of her clients, so this was a big problem for her.

A little research revealed what had probably happened: a person named Karen Rakow was named in some court papers, and an Internet search for "Karen Rakow" had turned up a link to a person with that name, who the slatkinfraud.com people proceeded to accuse. [RISK #1: Accusing person of a crime based only on similarity of their name to that of a real

suspect.]

[RISK #2: Trusting Internet searches to give semantically correct (and not merely textually similar) results.]

So Karen asked the slatkinfraud.com people to remove the references to her, her business, and her clients from their web site. They replied by saying they had done so, but in fact they had only removed some of the references.

Karen complained again, and they replied that "Our assistant webmaster has made another search and believes that all references to you and your company have now been removed from the site.

But we have 60 megabytes of material at slatkinfraud.com, so manual searches are not the most efficient way of doing this." [RISK #3: Using technology to build artifacts that are too large for you to manage.] [RISK #4: Making unverified modifications that you cannot easily undo.] Eventually all of the offending references were found and removed (we think).

Here is the really interesting part: the webmaster of slatkinfraud.com is a well-known computer scientist who definitely should have known better.

[RISK #5: Thinking that RISKS only apply to newbies.]

---

## **⚡ E-commerce website automatic response proves costly**

brian ally <b.ally@sympatico.ca>

*Fri, 01 Feb 2002 04:34:22 -0500*

The BBC has this story about Kodak giving in to customer's

demands that they honour a website promotion for cameras mistakenly listed for [much] less than they should have been. Seems their automatic e-mail response constituted an acceptance of the sale. As a Web developer, I'll certainly keep this in mind in the future.

[http://news.bbc.co.uk/1/hi/english/sci/tech/newsid\\_1795000/1795624.stm](http://news.bbc.co.uk/1/hi/english/sci/tech/newsid_1795000/1795624.stm)

---

## **Automated upgrade means no statistics**

Paul Roberts <Paul.Roberts@nautronix.com.au>

*Wed, 23 Jan 2002 13:19:08 +0800*

A report via APP that appeared on Australian IT (<http://australianit.news.com.au/articles/0,7204,3602608%5E15306%5E%5Enbv%5E,00.html>)

states that the Australian Bureau of statistics has been unable to provide data on people leaving or arriving in Australia (information collected on arrival/departure cards) for the last 18 months because of "technical difficulties" in upgrading from a manual to an automated system. This data is particularly useful to the tourism industry.

Apparently the "technical" difficulties are related to the outsourcing of the computer system. Hmm...sounds like there are more than "technical" difficulties, but unfortunately the outsourced company is not named.

## ⚡ Yet another Microsoft Outlook exploit

Bear Giles <bear@coyotesong.com>

Mon, 28 Jan 2002 22:31:26 -0700 (MST)

Yet another Microsoft Outlook exploit is on the loose... and this time the arrogance of the recommended solution is breathtaking. The problem is the built-in support for UUENCODED text within the body of a message. Prudent programmers will use a starting pattern such as

```
"\n\nbegin ([[ :octal: ]]+) ([^\n]+)\n"
```

and subsequently verify that each line has the expected format. Even checking only the first few lines (e.g., verifying that the first character correctly encodes the length of the rest of the line) essentially eliminates any chance of a false hit.

Sadly, it will surprise few people that Microsoft cuts straight to the heart of the matter. If your line starts with "begin " (possibly with two spaces), Outlook/Outlook Express WILL interpret the rest of the message as a UUENCODED attachment. It doesn't need a preceding blank line, nor a following octal number. It doesn't need subsequent lines that actually look like UUENCODED data.

There are some reports on slashdot that later versions of O/OE have discarded the "view source" command, with the effect that the rest of the message is permanently lost to the user. The use of this bug as

a DOS

attack on mailing lists that use a 'digest' approach is left as an exercise for the reader.

Naturally, it hasn't taken long for the malware writers to jump on the bandwagon. All you need to do to get around the "strip executable attachment" killjoys is to put the malware right in the body of the message!

Just start a line with "begin 666 www.myparty.yahoo.com" and you're off and running!

Microsoft's official position, at <http://support.microsoft.com/default.aspx?scid=kb;EN-US;q265230> , is

stunning in its <s>feeble-mindedness</s> simplicity. We, and by "we"

I mean every person on the planet who may ever send a message to an

O/OE <s>victim</s> user, or have a message forwarded to such users,

are advised (with editorial comments) to:

- \* not start messages with the word "begin"

(actually, it's \*any\* line starting with the word "begin". And

that's effectively a ban on the word "begin" for anyone using a

mail agent with transparent line wrapping, e.g., the web mail portals that some ISPs are pushing.)

- \* capitalize the word "begin," even when used within a sentence. E.g.,

"We will Begin the new project when Bob returns from his vacation.

- \* Use a different word such as "start" or "commence." E.g., all training materials for new Visual Basic programmers shall henceforce

refer to "start/end" loops instead of "begin/end" loops.

Microsoft's justification for suggesting a significant change to the English language instead of fixing their bug is given as:

"In a SMTP e-mail message, a file attachment that is encoded in UUencode format is defined when the word "begin" is followed by two spaces and then some data,..."

Needless to say there is no citation given for this "fact." That's probably related to the fact that UUENCODE was defined by UUCP, not SMTP, and that every encoder/decoder I have seen requires a leading blank line and a octal file permissions code.

But the damage is done - since malware is exploiting this bug we now get to put into place filters that don't just strip executable attachments or properly formatted UUENCODED blocks, we also have to strip *\*improperly\** formatted UUENCODED blocks!

Bear Giles

---

## ⚡ Bug in MS Excel?

Alberto <abit@wintermute.anu.edu.au>  
*Sat, 26 Jan 2002 15:08:16 +1100 (EST)*

Effect: Using database functions in Excel with autofilter on and hidden columns. Deleting rows will scramble the rows of the database.

How to see it:  
in Excel (all versions I tried fail) make a Database area, that

is,  
make a table with few rows and few columns, say 5 rows, 5  
columns for  
example. Fill it with whatever you want. Maybe fill the row 1  
with  
"c1", "c2", "c3", ... as those will be the names of the fields  
of the  
Database. Also, fill 1 column only with 0 and 1.

Select the table (with 1 more empty row) and define the name for  
the area  
"Database".

Chose the option AUTOFILTER ON, hide a column (not the one with  
0 and 1),  
using the automatic filter on the column with 0 and 1 ask for  
only the rows  
with 0 in that column.

Delete a row in the middle.

unhide the column that was hidden, remove the filtering and see  
that Excel  
did not delete the row in that column but did delete the row in  
the other  
columns.

Therefore the rows after the deleted one are all reporting  
misleading  
information.

I think this is serious. After some use the Database will be  
more or less  
scrambled.

Note that this would not happen if the autofilter was off  
regardless the  
number of hidden columns

Any advice?

Was this bug reported before?

Alberto <abit@maths.anu.edu.au>

---

## ✦ **Re: Excel cut-and-pasting behaviour (Brent, [RISKS-21.88](#))**

Peter Jeremy <peter.jeremy@alcatel.com.au>

*Tue, 29 Jan 2002 07:53:51 +1100*

About 40 years ago, Ed Lorenz re-ran a weather forecasting model using rounded figures and discovered Chaos Theory. Maybe Microsoft is hoping that Excel's (mis)behaviour will lead to an equally important discovery :-).

---

## ✦ **UK to try remote voting**

"Merlyn Kline" <merlyn@zyweb.com>

*Tue, 5 Feb 2002 17:42:16 -0000*

According to the BBC

([http://news.bbc.co.uk/1/hi/english/uk\\_politics/newsid\\_1802000/1802956.stm](http://news.bbc.co.uk/1/hi/english/uk_politics/newsid_1802000/1802956.stm)),

"Voters in Liverpool and Sheffield will be able to cast their ballot by sending a mobile phone text message in May's local elections." These elections will significantly empower real people as members of local councils.

Some more choice quotes from the article:

"The pilots will be crucial in building public confidence and testing

technical robustness to ensure that the integrity of the poll is maintained."

"In some wards in Liverpool and Sheffield voters will be able to cast their ballot by digital television as well as via their mobile phones."

"In Swindon there will be a touch-tone phone voting system, while Gateshead, North Tyneside, Stevenage and Chorley will pilot elections where people can only cast their ballot by post."

"The text messaging system will work by voters being given PIN numbers to use if they want to vote by text message."

"Opponents of online voting argue it is too easily exploited by electoral fraudsters..."

Endless potential RISKS discussed here previously may now be realised.  
Doubtless some new ones will come to light, too.

---

## 🔥 Miami-Dade OKs touchscreen voting

"David E. Price" <price16@ltnl.gov>  
*Wed, 30 Jan 2002 11:08:31 -0800*

Officials in Florida's Miami-Dade County have approved a \$24.5 million contract to replace the county's punch-card voting system with touchscreen equipment, in time for Nov 2002. The touchscreen machines make it impossible to vote for more than one candidate in each race, known as

overvoting, and alert voters if they fail to select any candidate, or undervote. Two other counties that were at the heart of the controversy -- Palm Beach and Broward -- also plan to use touchscreens. 30 Jan 2002 [source not specified]

[And as we have noted here before, today's touchscreen systems provide essentially ZERO hard evidence that your vote is counted as cast, and not for someone else or for no one. With just a little insider fraud, what a remarkable opportunity for rigging elections! PGN]

---

## **⚡ Re: Even unscientific elections get rigged (Epstein, [RISKS-21.87](#))**

Joe Thompson <joe@orion-com.com>  
*Sun, 27 Jan 2002 12:14:48 -0500*

This is really nothing new. The article Epstein linked to mentions the Microsoft "astroturf" campaign, but as early as the spring of 1998 a high-profile case of good-natured ballot stuffing was widely remarked upon: the People Magazine poll for Most Beautiful People. A campaign to write-in Howard Stern regular "Hank, the Angry Drunken Dwarf" had already boosted him to second place, until on 28 April 1998 Slashdot picked up the story and Hank shot to number one (by a margin of over 10 times his nearest rival). People played along to an extent, adding Hank as an official ballot choice,

but complaining about vote-stuffing.

That same spring I was witness to an episode more like Microsoft's effort.

The game company I worked for, Kesmai, had a game up for an online award

based on a reader survey. The director of the department that included

testing (the section I was in) instructed us to "vote early and often" until

Kesmai's offering topped the list. (Kesmai no longer exists, having been

bought by Electronic Arts in early 2000 and folded into the struggling

EA.com online game venture.)

All our effort was ultimately for naught, as by the next morning someone

\*else\* had apparently been hard at work stuffing the votes. We pondered

writing a Perl script but never did so.

The real risk in both of these cases is the assumption that a) one's own

poll is too small or specialized to attract a ballot-stuffing campaign or

b) that you can effectively detect rogue voters in an anonymous system.

---

## **⚡ Re: Woman says telephone makes unsolicited calls ([RISKS-21.88](#))**

"William Kucharski" <kucharsk@mac.com>

*Thu, 24 Jan 2002 07:00:26 -0700*

This is yet another in the "people treating Caller ID when the information

was never meant to be trusted" series.

As stated in past issues, anyone with a PBX system can program their system to deliver any given name and phone number as the CNID (Calling Number ID) information for any outgoing call from that system. In most businesses, this is used so that outgoing calls appear to be from that company's "main" number for incoming calls rather than from the actual phone line used to place the call.

A new trick many telemarketers are using to get around the new answering machines and phone company features that automatically shunt "Private" and "Out of Area" calls to telemarketer blocking features is to select a name at random out of the phone book and use that name and phone number for their outgoing CNID information. I know I regularly receive telemarketing calls that show up on my CID box as being from some person purported to be in the 619 area code...

This is no different from the way many spammers have recently taken to grabbing valid e-mail addresses and using those as "From" addresses for their missives. (I can't tell you the number of bounced e-mail reports I get for an e-mail address I stopped using some two or three years ago now, all with typical SPAM subject lines and originating from an open SMTP relay somewhere in the South Pacific.)

Alas, I don't believe misrepresentation of CNID information is any type of crime, as, as stated before, it was never meant to be secure or any type of

authenticated representation of who is actually calling...

RISKS: Believing that either CNID information or the "From" line on e-mail actually represent the true originator of the call or message in question...

---

## ✶ More Kaiser followup

Geoff Kuenning <geoff@cs.hmc.edu>

*Mon, 28 Jan 2002 14:31:03 -0800*

As a result of the recent discussion about security on the Kaiser Web site, my friend there has gone through the Web site registration process. In a previous private e-mail, she noted that the Medical Record Number (MRN) is not enough information to allow doing more than a few relatively innocuous things like checking appointment times. Here is her most recent message, outlining the results of the Web registration process:

```
> I received a letter in the mail including an activation code:
>
> (Dear...
> Thanks...)
> The PIN you've chosen will always let you into the site. The
next time you
> visit our site, we'll also ask you for your one-time
activation code.
>
> (Instructions)... It will start the more confidential
features of the Web
> Site, like answers to your personal health questions.
>
> We've sent you this Code by US Mail to make sure that no one
is pretending
```

> to be you online.  
>  
> (If you have problems.....)  
>  
> They never asked me for an address online so if the MRN and  
the name didn't  
> match or the address was wrong, this wouldn't have made it to  
me.

Sounds like Kaiser has actually done a pretty good job.

Geoff Kuenning    geoff@cs.hmc.edu    <http://www.cs.hmc.edu/~geoff/>

---

## **Re: REVIEW: "CISSP Examination Textbooks", S. Rao Vallabhaneni**

Rob Slade <rslade@sprint.ca>  
*Thu, 7 Feb 2002 11:04:02 -0800*

BKCISPET.RVW    20011122

"CISSP Examination Textbooks", S. Rao Vallabhaneni, 2000, , U  
\$213.00  
%A    S. Rao Vallabhaneni srvbooks@aol.com  
%C    P.O. Box 681354, Schaumburg, IL    60168-1354  
%D    2000  
%I    SRV Professional Publications  
%O    U\$99.00 per volume 847-330-0126 www.srvbooks.com  
%P    ~500 p. per volume  
%T    "CISSP Examination Textbooks" (vol 1 Theory, vol 2 Practice)

I should probably declare a bias. I am newly indoctrinated as a  
CISSP  
(Certified Information Systems Security Professional)  
instructor, so,  
presumably, anyone who decides to study for the exam out of a  
book, and not  
take the course, reduces my chances of getting assigned to teach

a course by  
approximately 0.016 percent.

Having said that, then:

These books will not help you study for or write the CISSP exam.

These books may, in fact, make your study more difficult, and  
your chances  
of passing the exam more remote.

At the very best, the time (and significant amount of money) you  
spend  
studying these books will be wasted, when you could have been  
reviewing  
other, more useful material.

If I went back through the files I might be able to find one,  
but, off the  
top of my head, I cannot recall a technical book with a poorer  
structure,  
organization, or grasp of the titular material. Many authors  
fail to do  
full research. A large number present the content in a  
disorganized manner,  
forcing the reader to do more work. Some have their own  
idiosyncratic  
definition of the topic, and may be slightly misleading in what  
they  
deliver. Seldom do the confluences of those aspects reach the  
depths of  
uselessness seen in these volumes.

While the (ISC)2 (International Information Systems Security  
Certification  
Consortium) CBK (Common Body of Knowledge) domain structure can  
be  
problematic, the "Theory" volume does not seem to follow either  
the (ISC)2  
study guide nor the CBK course outline. Point or section  
numbering is  
inconsistent, making it difficult even to follow the material.  
Tables and

illustrations are unclear, and either baldly repeat surrounding text, or have no relation to it. (Tables are often carelessly broken between pages, making reading of the charts and also surrounding text extremely difficult.) There are endless mistakes in spelling, grammar, and sentence or paragraph structure. Non-standard terms are used, and not defined. Occasionally small variations in phraseology seem to imply different topics that further (and pointless) study reveals to be identical. Major headings are sometimes simply printed, and are not explained or introduced. Certain topics and phrases are heavily emphasized, although not defined, and many of these are the most minor of issues in terms both of security and of the CISSP exam. Much of the technical material is confused, such as an analysis of the correspondence between "ISDN and OSI networks," which is something like comparing apples and juice extractors. The text contradicts itself frequently: a simple list of firewalls on one page does not relate to another three pages later. Some technologies have only one aspect explained, others are touched on without mentioning inherent dangers, others are so confused that closely related topics end up being set in opposition to each other. (The malware definitions, needless to say, are appalling.)

The "Practice" volume is a set of multiple choice questions supposedly similar to those you would encounter on the CISSP exam itself. Only those on the exam committee would be able to say, for certain, how close these

questions come to the real thing, but I can say that, in terms of information security, a great many of these questions simply make no sense.

The quality of the second volume seems to approximate that of the first.

I must say that, while the books and the Web site do carry a disclaimer that the tomes are not endorsed by (ISC)2, I am slightly appalled that (ISC)2 has not objected to the use of this particular name. In fact, these books appear on the (ISC)2 resource list. Which, itself, carries a disclaimer that such a listing does not imply any endorsement. Even so, the simple association gives the work a cachet that is wholly undeserved, and probably misleading. (I should also note that, as a relatively new CISSP I don't have a solid idea of how the books on the reference list at <https://www.isc2.org/cgi-bin/content.cgi?page=36> got there.)

I should also note, in strict fairness, that one of my fellow instructors used these books and self-study to pass his own exam, and said that he found them very useful.

But, in my own opinion, and at the risk of repeating myself, if you are studying for the CISSP:

Do not buy these books.

If you have bought these books, do not read them.

copyright Robert M. Slade, 2001    BKCISPET.RVW    20011122  
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 21: Issue 91**

**Weds 13 February 2002**

## Contents

- [Microsoft C++ feature against buffer overflows itself vulnerable](#)  
[Gary McGraw](#)
- [Hole found in Net security program](#)  
[Bill Hopkins](#)
- [Security flaw in Sony Vaio computers](#)  
[Monty Solomon via Dave Farber](#)
- [Computer controller crane goes wrong](#)  
[Jeff Jonas](#)
- [Election risks from lack of randomization](#)  
[Keith Price](#)
- [Search engines may give you the wrong e-mail address](#)  
[Robert Marshall](#)
- [Hotel Internet access](#)  
[Christian Holz](#)
- ["Secure" credit-card transactions with new Amstrad e-mailerplus](#)  
[Merlyn Kline](#)
- [Officer calls for refund of 'speeding' fines](#)  
[Monty Solomon](#)
- [Risks of the rise of PowerPoint](#)  
[Andrew Main](#)

- [Microsoft and English](#)  
[Toby Gottfried](#)
  - [Re: Bulgarian parliament against weight loss](#)  
[Valentin Razmov](#)
  - [Bill payer system silently changes payments](#)  
[Phil Weiss](#)
  - [Social Security Numbers printed on tax envelopes](#)  
[Steve Klein](#)
  - [Virus writers aren't playing fair](#)  
[William Colburn](#)
  - [Re: Homograph risks](#)  
[Merlyn Kline](#)
  - [Survey finds security lax at nonprofits](#)  
[Audrie Krause](#)
  - [REVIEW: "Zimmerman's Algorithm", S. Andrew Swann](#)  
[Rob Slade](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

## ⚡ Microsoft C++ feature against buffer overflows itself vulnerable

"Gary McGraw" <gem@cigital.com>

Wed, 13 Feb 2002 12:57:03 -0500

Microsoft added a new security feature to their latest C++ compiler, called both Visual C++.Net and Visual C++ version 7, that was released 13 Feb 2002. This security feature is meant to protect potentially vulnerable source code automatically from some forms of buffer overflow attack. The protection afforded by the new feature allows developers to continue to use vulnerable string functions such as strcpy() as usual and still be "protected" against some forms of stack smashing. The new feature is closely based

on an invention of Crispin Cowan's StackGuard and is meant to be used when creating standard native code (not the new .NET intermediate language, referred to as "managed code").

Note that the new feature is meant to protect any program compiled with the "protected" compiler feature. In other words, the idea is that using this feature should help developers build more secure software. However, in its current form, the Microsoft feature leads to a false sense of security because it is easily defeated. An ironic RISK, to be sure.

Microsoft's feature includes the ability to set a "security error handler" function to be called when a potential attack is underway. Because of the way this was implemented, the Microsoft security feature is itself vulnerable to attack. An attacker can craft a special-purpose attack against a "protected" program, defeating the protection mechanism in a straightforward way.

There are several well known approaches not based on StackGuard that a compiler-producer might use to defeat buffer overflow attacks. Microsoft chose to adopt a weak solution rather than a more robust solution. This is a design-level flaw leading to a very serious set of potential attacks against code compiled with the new compiler. The Microsoft compiler is thus in some sense a "vulnerability seeder".

More technical information about the flaw can be found at <http://www.cigital.com/news/mscompiler-tech.html>

The flaw was discovered by Chris Ren, a Cigital Labs researcher. Microsoft has been alerted to the flaw and plans to address it in future VC releases.

Gary McGraw, Ph.D., CTO, Cigital

---

## 🔥 Hole found in Net security program

"Bill Hopkins" <whopkins@wmi.com>

*Fri, 8 Feb 2002 19:18:39 -0500*

In case you haven't seen it... I'm sure you'll hear from others who are likely more familiar with the product.

<http://www.nytimes.com/aponline/technology/AP-Computer-Security.html>

Quick summary: BlackICE Defender and BlackICE Agent have a security hole involving, yes, buffer overflow. Once through the firewall, guess who's in charge?

A download fixes it.

---

## 🔥 Security flaw in Sony Vaio computers (from Monty Solomon)

David Farber <dave@farber.net>

*Sat, 26 Jan 2002 17:51:43 -0500*

TOKYO: Japan's Sony issued a warning on Thursday after finding a

software

problem in a popular range of computers that could expose around 900,000

customers to attacks from hackers. [...]

[http://www.timesofindia.com/articleshow.asp?art\\_id=473172674](http://www.timesofindia.com/articleshow.asp?art_id=473172674)

---

## **⚡ Computer controller crane goes wrong**

"Jeff Jonas" <jeffj@panix.com>

*Sun, 10 Feb 2002 04:01:49 -0500 (EST)*

Jersey City NJ, 16 Jan 2002: A computer controlled/assisted crane got into an unstable position, requiring the evacuation of nearby apartments for 2 days now.

RISKS follows when airplanes and trains surrender control from people to computers. Now add construction cranes.

---

## **⚡ Election risks from lack of randomization**

Keith Price <price@usc.edu>

*Tue, 12 Feb 2002 11:34:39 -0800 (PST)*

At first I did not think it was a computer risk. I'm still not sure if it is, but the random order list is computerized.

The Mayoral election (Nov 2001) in Compton, CA was overturned (8 Feb 2002)

because of the random ordering of names on the final ballot. The local

clerk had not requested a new randomized order from Sacramento, and had used the same order as in the earlier primary election. The Judge decided that the 300-vote margin was less than the advantage due to being listed first rather than second and reversed the counted results. So, in California they will count your vote, but your vote may not count.

---

## **✂ Search engines may give you the wrong e-mail address**

"Robert Marshall" <robert@chezmarshall.freemove.co.uk>

*Tue, 12 Feb 2002 13:33:31 +0000*

I was searching for the work e-mail address for a friend using google.

Let's say the name was Paul Consultant. Google gave me a hit with the

correct company and the web page was such that his e-mail appeared in

the google summary. So I cut and pasted it directly without having to

visit the company web site. It appeared as PR.

Consultant@relations.com.

When the e-mail bounced I investigated and the company web page has the

mail as P.R.Consultant@relations.com, as does google's cache. It looks as if

google is trying to cut down on the synopsis by removing redundant '.'s

Unfortunately they aren't always redundant. Fortunately my e-mail bounced

rather than going to an unrelated recipient.

## **✶ Hotel Internet access**

Christian Holz <chrish@thewizardry.com>

*Mon, 11 Feb 2002 01:30:18 +0100*

I have just found out about an interesting feature of STSN Internet Access, common at hotels in the New England area. They have little boxes connected in each room which provide either full-fledged Ethernet access, USB or Modem connections.

To make it especially easy for users, they re-route packets based on the service used(!). When I tried to connect to my SMTP server (which uses SMTP-AUTH to protect against Spamming), I got a message informing me that the used SMTP server does not provide SMTP-AUTH. After a short heart-attack that my server has been hacked, I telnetted to my SMTP-Server and I was connected to STSN's.

The risk: Obvious, if they can re-direct based on the service used, they could possibly see a lot of passwords by providing proxy-services for common services. In addition with the hotel-guest information, this could give an interesting profile of hotel guests. I wonder what information they can get their hands on if they have this services in Capitol-Hill hotels...

I am using SSH-tunnels from this day onwards...

## **✶ "Secure" credit-card transactions with new Amstrad e-mailerplus**

"Merlyn Kline" <merlyn@zyweb.com>

*Fri, 8 Feb 2002 15:53:01 -0000*

Amstrad (<http://www.amstrad.com/>) in the UK have announced their new Internet appliance, the e-mailerplus. Among other features, this includes a "built in a SMARTCARD reader to enable Secure Credit Card Transactions in the future". Given that there is no extant standard for this sort of thing, I wondered how this would work. The answer is quickly found on their web site:

"The e-mailerplus has all the necessary hardware required to enable this additional level of security ALREADY BUILT-IN and it is only a matter of delivering the software code to the machine remotely, which we will do, as and when it is developed."

"We will be developing software in conjunction with this secure payment system which will be downloaded automatically to the entire population of this machine at NO cost to the user."

RISKS readers will no doubt wonder what other code might be downloaded, by whom, and for what nefarious purposes.

---

## **✶ Officer calls for refund of 'speeding' fines**

Monty Solomon <monty@roscom.com>

*Sun, 10 Feb 2002 23:56:39 -0500*

HARTFORD - A hearing officer for the state Department of Consumer Protection recommended yesterday that a New Haven rental car company be ordered to refund the ''speeding'' fines it levied after tracking customers with satellites. Hearing officer Robert H. Brinton Jr. also recommended that Acme Rent-a-Car be prohibited from fining customers in the future. The company had used global positioning system satellites to track its cars and had fined renters \$150 each time a car exceeded 79 mph for more than two minutes. ... [Source: Associated Press, 8 Feb 2002]  
[http://www.boston.com/dailyglobe2/039/metro/Officer\\_calls\\_for\\_refund\\_of\\_speeding\\_fines+.shtml](http://www.boston.com/dailyglobe2/039/metro/Officer_calls_for_refund_of_speeding_fines+.shtml)

---

## **✶ Risks of the rise of PowerPoint**

Andrew Main <zefram@fysh.org>

*Sun, 10 Feb 2002 23:09:54 +0000*

There was an interesting radio program today discussing the influence of the PowerPoint program on business ("In Business", BBC Radio 4, 2002-02-10 21:30). One of the presenter's main points was that the use of PowerPoint has affected the way businesses operate: not only are slides now used so much that each presentation revolves around its slides, rather than vice

versa, but also apparently PowerPoint now has a Content Wizard, that provides templates for certain types of presentation.

There were reports of PowerPoint users sticking religiously to the format of the template, as the canonical way to organise a presentation. The PowerPoint developer who was interviewed sounded somewhat embarrassed by the phenomenon: she said "~we expected people to modify those presentations a great deal~" (approximate quote). The main risk here is familiar: users blindly accepting whatever default the computer provides, without considering whether it's appropriate ([RISKS-7.57](#), et al.). In this context, rather than doing anything sufficiently incorrect to make things obviously fail, the inappropriate defaults are having a subtle influence on businessmen's thinking (slides titled "our vision for the future" and so on).

Really the risk is a more general informational one -- people misunderstanding the purpose and intent of a piece of information, or often misunderstanding which source of information is authoritative. We have the same class of problem when humans talk to humans -- how many people will call their bank and ask "please change my address" rather than "please note my change of address"? The obvious solutions are also human/informational ones: clearer thinking about these issues on the part of the receivers of information, and on the other side clearer labelling of the intent of information.

Andrew Main <zefram@fysh.org>

## ⚡ Microsoft and English

"Toby Gottfried" <toby6700@earthlink.net>

*Sun, 10 Feb 2002 11:57:39 -0800*

In [RISKS-21.90](#), Bear Giles writes about Microsoft "appropriating" the word "begin" in e-mail messages to denote UUENCODEd text.

"Microsoft's justification for suggesting a significant change to the

English language instead of fixing their bug is given as:"

Riding roughshod over some little used trifle like the English language is

not a big deal to an important technology innovator like Microsoft. They

did just that by naming a major project dot-Net (".Net").

Before that, a

period followed by a capital letter was used to mark a sentence boundary.

Experienced readers of English will note a brief interruption in their

parsing whenever .Net is encountered mid-sentence. And they will be annoyed

about it.

---

## ⚡ Re: Bulgarian parliament against weight loss (Larmour, [RISKS-21.88](#))

Valentin Razmov <valentin@cs.washington.edu>

*Tue, 22 Jan 2002 21:19:22 -0800 (PST)*

> weighing scales set into the seat

While the proposed improvement does have its downsides, the alternative suggestion for using personalized cards would \*not\* work as it misses the main point the system is trying to solve (and the biggest problem of the previous system) - preventing collusion.

(MPs have been known to give their cards to colleagues while absent from the plenary hall, which creates the danger of passing laws without even having quorum among voting MPs.)

Cards (whether personalized or not) are capabilities, possibly with some form of authentication "attached" to defeat theft, but certainly not to defeat collusion - if I want to give you my card, I could just as well tell you my secret code for "activating" it.

Hence biometrics come to mind as a form of authentication that prevents collusion in our case without the need for a designated parliament secretary looking over MPs' shoulders.

Weighing scales offer a degree of protection at a very low cost. The system does allow both false positives (non-malicious MPs unable to vote because of a sudden difference with their established weight) and false negatives (dishonest MPs casting a vote not only for themselves), and while this does not guarantee that glitches won't happen, it also makes premeditated malice somewhat harder to carry out.

Alternative schemes would have their own tradeoffs and it is not immediately

clear if any of them would be any more cost-effective. (The low-tech version of MPs standing in line to cast physical ballots every time they need to vote is about as fool-proof as can get, but not very efficient.)

Valentin

Full disclosure: I am Bulgarian, but I did not know about the new system until reading the news.

---

## ✶ Bill payer system silently changes payments

Phil Weiss <philsjunkmail@yahoo.com>  
*Tue, 22 Jan 2002 21:01:43 -0800 (PST)*

I use First Tech Credit Union's (<http://www.1sttech.com/>) online bill payer system. As is typical for many financial institutions, the processor is not First Tech itself, but instead a company called Princeton ECom (<http://www.princetonecom.com/>).

The system works by having the user select a payee, then having the user enter in the due date for the bill along with the amount. If the processor can pay the bill using electronic funds transfer (EFT), the system subtracts 3 days from the date entered and uses that for the day money will be withdrawn from your account and the payment sent. If the processor cannot pay using EFT, it subtracts 8 days from the due date and uses that instead. It then presents a confirmation page.

I found out recently a couple of risks (in addition to some known ones with their system). When my December payment was late, I looked at the status of the payment and was surprised to see that it had silently been changed to "check" from "electronic." Since it had been scheduled 3 days before the due date but was now sent by check, it arrived several days late.

When I inquired to the credit union they gave me several explanations. The processor recently began requiring the account number that is entered for my mortgage company to be a 10 digit number (0001234567 instead of 1234567). At the same time the mortgage company changed it's "make checks payable to" name from Mortgage Service Center back to PHH Mortgage Services (they've switched this several times on me over the years).

They will make that change silently without warning the user if you change anything about the payee to break the match of your payee info to their list of EFT payess. And if they make a change to the payee due to a change in policy, it will change your payment methods without notifying customers that they need to update their pending payments. It isn't really a risk, it's a certainty of errors.

The risk on my part was assuming the system would work. Being a software developer by trade, it's something I shouldn't have assumed. I've since changed all the important payments so that the due dates are at least a half a month ahead of their due date. If I don't see the money deducted from my

account, I can take substitute action. (For things like my newspaper subscription, I don't really care.)

---

## **✶ Social Security Numbers printed on tax envelopes**

Steve Klein <steveklein@mac.com>

*Tue, 29 Jan 2002 08:47:37 -0500*

The city of Detroit, Michigan has sent out 400,000 income tax forms with taxpayers' social security numbers printed on the outside of the envelopes.

City officials were unable to explain why the numbers were included on the forms or how the printer got them.

Ralph Kinney, deputy chief of the Wayne County Sheriff's Department's High-Tech Crime Unit, said names, addresses and Social Security numbers are the main targets of identity thieves.

"Social Security is really the key to unlocking a person's credit identity," Kinney said. "If that key falls into the wrong person's hand, it makes it a lot easier for someone to become that person."

Identity theft, a felony in Michigan, is one of the fastest-growing white-collar crimes, Kinney said.

Dennis Ertzbischoff, a local citizen who was one of those affected said,

"This is the kind of mistake a first-year programming student would make.

This was sheer stupidity. Nobody reviewed the work, and nobody

caught it."

(Excerpted and paraphrased from the Detroit Free Press, 2002-01-29.)

Steve Klein, Your Mac Expert, Phone (248) YOUR-MAC-EXPERT (or 248-968-7622)

---

## ✈ Virus writers aren't playing fair

"Schlake ( William Colburn )" <schlake@nmt.edu>

*Mon, 28 Jan 2002 15:53:36 -0700*

Today I got a weird e-mail with some inline uuencoded data that had a filename of www dot myparty dot yahoo dot com. My McAfee didn't detect it as a virus, but it uudecoded into a DOS executable so I was suspicious. I sent it off to McAfee, and they sent me back an EXTRA.DAT for it. Then came the real trouble.

I use a milter I wrote (<http://www.nmt.edu/~wcolburn/antivirus/>) to detect viruses. Up until today, it had used error codes to know if a file needed scanning. The mail file would be "ripmime"ed, and if the error code was 0 (no error) then it meant that some files were successfully extracted. If files were extracted then they needed to be scanned.

This new virus, W32/Myparty (ED), defeated me on several levels. The virus wasn't MIME encoded, so ripmime didn't find it. I added a blind uudecode to my milter, but it was defeated as well. The uuencoded virus is "corrupt"

(but it creates some output which runs), so the return code from the uudecode command indicates (is indistinguishable from) nothing decoded.

In the end, I decided that the best thing to do is to blindly uudecode AND ripmime AND scan every single message. As you can imagine, this is a terrible solution. The core of the problem stems from the fact that MS products seem to "be generous in what they accept" (the way all good software should be written?), and so they don't care that the mail wasn't MIME encoded, nor that it contained a corrupt file.

The risk is that systems are so complex it is getting increasingly hard to protect them. That virus shouldn't propagate because it isn't MIME encoded, but it does. That virus shouldn't propagate because it uses a corrupt file transfer, but it does. If both things were done on purpose, then the writer was clever. I can image that more software writers than myself considered "garbage" or "corrupt" data as "safe".

---

## ⚡ Re: Homograph risks ([RISKS-21.89](#))

"Merlyn Kline" <merlyn@zyweb.com>

*Wed, 30 Jan 2002 09:47:31 -0000*

> For example, a Russian "o" and an English "o" look alike ...

The default font chosen by Microsoft for some of their desktops (e.g.,

Windows NT) contains homographs for lowercase L and uppercase i. I've suffered from minor problems arising from this and I can imagine bigger risks.

Worse, the default font used by many of their code editors used to contain homographs for lowercase L and the number 1. I learnt this the hard way, staring at broken code that was \*obviously\* correct! I've long since acquired the habit of using a non-standard font for code editing so I can't say whether the latest versions of their fonts still have this problem (which is presumably inherited from the historical use of lowercase L as the number 1 on many typewriters).

[Backwards compatibility is either a pun or an oxymoron. PGN]

---

## **Survey finds security lax at nonprofits**

Audrie Krause <audrie@netaction.org>

*Wed, 30 Jan 2002 11:26:45 -0800*

We've just released the results of NetAction's survey of security practices in nonprofit organizations. I thought it might be of interest to RISKS readers.

Despite the growing importance of computers to nearly every aspect of nonprofit operations, an online survey of security practices in nonprofit organizations found substantial room for improvement, especially in maintaining the security of confidential and/or sensitive files,

user work habits, and disaster planning.

"Nonprofit organizations are just as vulnerable to cyber attacks as businesses and government agencies," said NetAction executive director Audrie Krause. "This should be a wake up call to the nonprofit sector: security needs to be improved."

NetAction's report on the survey results, "Computer Practices in Nonprofit Organizations," is available at: <http://netaction.org/security/>.

Many of the respondents acknowledged the need to improve their security practices. When asked to identify specific security issues their organization needs to address, about two-thirds of the survey respondents listed user work habits and disaster planning, about half listed data backups and encryption, and about one third listed virus protection and firewalls.

The need to improve the security of confidential and/or sensitive files (such as personnel records or financial documents) was especially evident. Only 4% of nonprofit organizations encrypt all sensitive files. Yet nearly two thirds of the organizations surveyed store sensitive files on computers connected to a local network, and nearly half store them on computers connected to the Internet.

Moreover, computer users in nearly one fourth of the organizations that NetAction surveyed do not routinely lock or shut down their computers when they are away from their desks, and 80% of the nonprofits indicated that

volunteers, interns, outside consultants and/or temporary staff have access to office computers.

"Some risks aren't as obvious as others," said Krause. "Most organizations are aware that they could lose important data if they don't do regular backups. But they may not realize that when users forget to logoff, a disgruntled employee could steal confidential information, or a nosy volunteer could access an organization's personnel records."

NetAction's survey also found that only slightly more than half of the nonprofit organizations back up their data every day, and only about one third have a data recovery plan in the event of catastrophic data loss.

The organizations did a somewhat better job of protecting their computers from viruses. About two-thirds of the organizations updated their anti-virus software one or more times per month. However, the survey also found that about two-thirds of the nonprofits use Microsoft's Outlook or Outlook Express to send and receive e-mail despite the higher risk of an attack by viruses or worms than with other e-mail clients.

The online survey was conducted between December 19, 2001 and January 20, 2001. Although the results cannot be generalized to the larger nonprofit community because random sampling techniques were not used, Krause said nonprofit organizations should find the report useful in assessing their own computer security practices and identifying practices that need improvement.

[...]

She added, "Security experts were concerned about the vulnerability of computer systems to cyber attacks long before the horrendous events of September 11, 2001; the level of concern has only increased since the terrorist attacks on New York City and the Pentagon. [...]"

NetAction, Audrie Krause, Exec.Dir., 601 Van Ness Ave., No. 631, San Francisco  
CA 94102 1-415-775-8674 <http://www.netaction.org>  
audrie@netaction.org

---

## 🔥 REVIEW: "Zimmerman's Algorithm", S. Andrew Swann

Rob Slade <rslade@sprint.ca>  
*Tue, 12 Feb 2002 07:56:32 -0800*

BKZIMALG.RVW 20011126

"Zimmerman's Algorithm", S. Andrew Swann, 2000, 0-88677-865-4  
%A S. Andrew Swann (Steven Swiniarski)  
%C 375 Hudson Street, New York, NY 10014  
%D 2000  
%G 0-88677-865-4  
%I DAW Books Inc.  
%P 387 p.  
%T "Zimmerman's Algorithm"

A thriller should have a convoluted plot, but this one has slightly too many twists and turns for comfort. It's very difficult to keep track of at least three sets of bad guys, and by the time the penultimate plot is exposed I had a hard time caring who was responsible. Still the action is

brisk, and  
the writing is lively and interesting.

So is the fact that so much technology in the story is basically correct.

The outcomes are sometimes questionable, such as a computer made with

superconducting materials that physically (and not just electrically)

degrade at room temperature. But the fact that researchers developing

artificial materials are steadily working towards room temperature

superconductors is true.

The math isn't that bad, either. There is a slight overemphasis on the need

for primes in encryption systems, but it is interesting to see a recognition

of the controversy over enormous computer generated proofs.

The computer work is a bit weaker. Genetic algorithms are not terribly well

explained in the computer world in general, so it isn't surprising that the

detail in the book is a bit fuzzy. The discussion of computer viruses as a

form of artificial life is interesting, as is the view of benignity as a

survival factor, although the idea of masses of undetected viruses hiding

out on the Internet is a bit much. (I must say, though, that, if you are

going to propose the usual undetectable virus, one that can write operating

systems is a good candidate.)

I would like to know whether the choice of name for the eponymous mathematician was influenced by PGP.

copyright Robert M. Slade, 2001 BKZIMALG.RVW 20011126  
rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca  
pl@canada.com

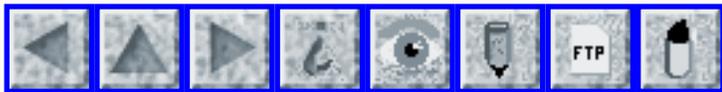
[http://victoria.tc.ca/techrev  
~rslade](http://victoria.tc.ca/techrev/~rslade)

or

<http://sun.soci.niu.edu/>



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 21: Issue 92**

**Weds 20 February 2002**

## Contents

- [Patriot misses again](#)  
[Lord Wodehouse](#)
- [Researchers claim to crack Wi-Fi security](#)  
[Monty Solomon](#)
- [When machine metadata fails, address humans](#)  
[Diomidis Spinellis](#)
- [Unwitting cell calls swamp 911 systems](#)  
[Monty Solomon](#)
- [Abuse of intercept capabilities: 'Tampa' affair](#)  
[Geoffrey Brent](#)
- [PayPal's tenuous situation](#)  
[Jeff Jonas](#)
- [Ice-skating judging solution](#)  
[Ken Knowlton](#)
- [Re: Miami-Dade OKs touchscreen voting](#)  
[Alan Brain](#)
- [An unlocked system can be compromised quickly](#)  
[Greg Searle](#)
- [Dangerous characters](#)  
[Mark Lomas](#)

- [Computerized assistance with non-standard punctuation](#)  
[David Piper](#)
  - [Re: Homograph problems](#)  
[Geoffrey Brent](#)
  - [What's a buffer overrun problem?](#)  
[William P. N. Smith](#)
  - [Sorry, that number is now in service](#)  
[Gene Spafford](#)
  - [Re: Officer calls for refund of 'speeding' fines](#)  
[Henry Baker](#)
  - [Re: Social Security numbers on tax envelopes](#)  
[Robert Ellis Smith](#)
  - [The Security Risks of Programs That Automatically Update](#)  
[Scott Schram](#)
  - [New Security Conference - GOVSEC, Call for Presentations](#)  
[Jack Holleran](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

## ✶ Patriot misses again

Lord Wodehouse <w0400@ggr.co.uk>

*Tue, 19 Feb 2002 11:06:49 +0000 (GMT Standard Time)*

The long running saga of the Patriot missile continues.  
Spacedaily reports  
(<http://spacedaily.com/news/020217211535.6h8kn7ih.html>) that two  
of three  
missiles fired recently at White Sands under "battlefield  
conditions" with  
three targets failed to intercept them.

... and someone wants to build a missile defence system ... (and  
if you  
still think it is a good idea, check back through the RISKS  
archives)

John, SCS Global Services, GlaxoSmithKline, Medicines Research Centre,  
Gunnels Wood Road, Stevenage SG1 2NY UK +44 1628 482 634 <http://www.gsk.com/>

---

## ✦ Researchers claim to crack Wi-Fi security

"monty solomon" <monty@roscom.com>

*Fri, 15 Feb 2002 12:24:10 -0500*

Ephraim Schwartz, InfoWorld, Thursday, February 14, 2002  
Researchers Claim to Crack Wi-Fi Security;

Proponents deny wireless networking spec is vulnerable to hijack,  
authentication attacks.

<http://www.pcworld.com/news/article/0,aid,84424,00.asp>

A University of Maryland professor and his graduate student have apparently uncovered serious weaknesses in the next-generation Wireless Fidelity security protocol known as 802.1x. In a paper, "An Initial Security Analysis of the IEEE 802.1X Standard" funded by the National Institute of Standards, Professor William Arbaugh and his graduate assistant Arunesh Mishra outline two separate scenarios that nullify the benefits of the new standard and leave Wi-Fi networks wide open to attacks. The use of public access "hot spots" are particularly vulnerable to session hijacking because these locations do not even deploy the rudimentary Wired Equivalent Privacy protocol. "This problem exists whether you use WEP or not, but it is trivial to exploit if not using WEP," said Arbaugh.

## Flaws Described

Dubbed "session hijacking" and "man-in-the-middle," both attacks basically exploit inherent problems in Wi-Fi as well as exploiting how the new 802.1x standard is designed. "Here's how session hijacking works. The hacker waits for someone to finish successfully the authentication process. Then you as the attacker send a disassociate message, forging it to make it look like it came from the AP [access point]. The client [user] thinks they have been kicked off, but the AP thinks the client is still out there. As long as WEP is not involved you can start using that connection up until the next time out, usually about 60 minutes," said Arbaugh. [...]

[Fine article. Well worth reading The Rest of the Story. PGN]

---

## ✶ When machine metadata fails, address humans

Diomidis Spinellis <dds@aueb.gr>

*Tue, 19 Feb 2002 15:16:20 +0300*

The aggressive indexing of the Google search engine combined with the on-line caching of the pages in the form they had when they were indexed, is resulting in some perverse situations.

A number of RISKS articles have already described how sensitive data or supposedly non-accessible pages leaked from an organization's intranet or web-site to the world by getting indexed by Google or other

search engines.

Such problems can be avoided by not placing private information on a publicly accessible web site, or by employing metadata such as the robot exclusion standard to inform the various web-crawling spiders that specific contents are not to be indexed. Of course, adherence to the robot exclusion standard is left to the discretion of the individual spiders, so the second option should only be used for advisory purposes and not to protect sensitive data.

Today I came across a web page <<http://www.rietta.com/sqlconnect/>> with metadata addressing the humans reading a page rather than the spiders. The page was apparently inadvertently, from the company's point of view indexed by Google:

"NOTE: This page has been picked up by Google before we intended for it to become visible. The SQL Connect software is completed, but we still have to finalize the documentation and this website in order to release it. Please check back soon for the download, or if you have questions, you can e-mail [products@rietta.com](mailto:products@rietta.com)."

Worryingly, the same company also markets RoboGen, a product to manage the robot exclusion specification file: "RoboGen allows you to easily manage a robot exclusion file to control search engines indexing your website.

Featured in magazines and books, RoboGen is the most popular and easy to use program for managing search engines that visit your website."

The moral? The web has a long (and growing, see <http://www.archive.org>) memory. Information leaks due to incorrect spider metadata and other errors can only be partially contained by addressing new metadata to humans.

Diomidis Spinellis - <http://www.dmst.aueb.gr/dds/>  
Athens University of Economics and Business (AUEB)

---

## ✶ Unwitting cell calls swamp 911 systems

Monty Solomon <monty@roscom.com>

*Wed, 20 Feb 2002 18:46:02 -0500*

Unwitting Cell Calls Swamp 911 Systems,  
By JILL LEOVY, Los Angeles Times, 19 Feb 2002

Frustrated by the large volume of 911 calls caused by people accidentally hitting programmed buttons on their cell phones, police and emergency response authorities are seeking new ways to keep systems from becoming overloaded. Nearly two-thirds of all the 911 calls from wireless phones in California, and even higher proportions elsewhere in the country, involve people pushing emergency buttons on their cell phone keypads without knowing it, authorities say.

<http://www.latimes.com/technology/la-000012715feb19.story>

---

## ✶ Abuse of intercept capabilities: 'Tampa' affair

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

Thu, 14 Feb 2002 15:25:01 +1100

Last year, shortly before a federal election, the ship 'Tampa' made Australian headlines when it rescued a boatload of about 400 refugees off the Australian coast. A controversy followed on whether Australia would be obliged to give the 'Tampa' harbour and accept said refugees.

It has recently been alleged that Australia's Defence Signals Directorate (DSD) intercepted communications between the skipper of the 'Tampa' and the Maritime Union of Australia and passed this information on to government. By law the DSD is banned from intercepting Australian communications (with certain exceptions not relevant here).

The Defence Minister, Robert Hill, has issued a very carefully-worded response: there were "no significant breaches" of these rules, and guidelines designed to protect privacy were adhered to "in the broad". While denying that MUA communications were intercepted, Hill conceded that the DSD had broken its rules relating to spying on Australians. Hill has given assurances that the breach was not a major one, but without any information on the nature of the breach confirming that is another matter...

[http://www.theaustralian.news.com.au/common/story\\_page/0,5744,3766399%255E601,00.html](http://www.theaustralian.news.com.au/common/story_page/0,5744,3766399%255E601,00.html)

<http://www.abc.net.au/am/s480125.htm>

<http://www.smh.com.au/news/0202/14/national/national3.html>

et al.

Since the Tampa crisis played a very major role in the resurrection of the Howard government's political fortunes, quite likely altering the outcome of last year's federal election, the possibility of illegally-obtained intercepts being used for political ends is not being taken lightly by anybody (except, perhaps, that government...)

Geoffrey Brent

---

## ✶ PayPal's tenuous situation

"Jeff Jonas" <jeffj@panix.com>

*Sun, 10 Feb 2002 06:38:08 -0500 (EST)*

PayPal is much in the news after their NASDAQ IPO was further delayed due to a lawsuit filed by CertCo concerning patent infringement. (the risk of frivolous software patents had been discussed before in RISKS).

More damning in my eyes are the problems PayPal had to reveal in their prospectus and the lack of discussion I've seen about the failures:

Their prospectus is found at:

[http://www.edgar-online.com/bin/edgardoc/finSys\\_main.asp?dcn=0000912057-01-543278](http://www.edgar-online.com/bin/edgardoc/finSys_main.asp?dcn=0000912057-01-543278)

It's interesting reading: they admit that they've never made any profit, might never make a profit, and all the ways they might be squeezed out of business.

> AMENDMENT NO. 2 TO FORM S-1 REGISTRATION STATEMENT  
> UNDER THE SECURITIES ACT OF 1933 PAYPAL, INC.

> We have not reached profitability to date.  
> We have accumulated net losses of \$264.7 million  
> from our inception, March 8, 1999, through September 30, 2001,  
> and net losses of \$90.6 million during the nine months  
> ended September 30, 2001.

> During the four months between July and October 2000,  
> we experienced a significant fraud episode and, as a result,  
> we incurred gross losses due to unauthorized charge-backs  
totaling  
> \$5.7 million. This amount represented 64.0% of total charge-  
backs  
> due to unauthorized transactions for the year ended December  
31, 2000.

Ummm, what was done to prevent this fraud from recurring?  
Anyone caught? Anything learned?

> For the year ended December 31, 2000, the amount of losses  
> with respect to unauthorized use of bank accounts totaled \$0.3  
million.  
> The gross amount of charge-backs received through September  
30, 2001  
> with respect to unauthorized use of credit cards for  
transactions  
> that occurred during the nine months ended September 30, 2001  
> totaled \$3.2 million. For the nine months ended September 30,  
2001,  
> the amount of our losses with respect to unauthorized use of  
> bank accounts totaled \$0.9 million.

Gee, where do I get my share?

> We may experience breakdowns in our payment processing system  
> that could damage customer relations and expose us to  
liability,  
> which could affect adversely our ability to become profitable.

So why not act proactively with better failsafes such as having 2  
active/active sites, automatic load balancing to shift the load

in case of failure, etc. All things available to buy and implement NOW!

> A system outage or data loss could have a material adverse effect on our

> business, financial condition and results of operations.

> To operate our business successfully, we must protect our payment processing

> and other systems from interruption by events beyond our control.

> Events that could cause system interruptions include:

> \* fire;

> \* earthquake;

> \* terrorist attacks;

> \* natural disasters;

> \* computer viruses;

> \* unauthorized entry;

> \* telecommunications failure;

> \* computer denial of service attacks; and

> \* power loss and California rolling blackouts.

> We depend on two third parties for co-location of our data servers

> and rely upon these third parties for the physical security of our servers.

> Our servers currently reside in facilities in Santa Clara, California.

All your eggs in one basket: power failure, telecom failure, etc are all totally fatal.

> Currently we are not able to switch instantly to another back-up site

> in the event of failure of the main server site.

> This means that an outage at one facility could result in our system being

> unavailable for at least several hours. This downtime could result in

> increased costs and lost revenues which would be detrimental to our business.

I see no excuse for that since quality of service load balancing routers exist

specifically for such protection.

- > Our primary Internet hosting provider, Exodus, recently filed for protection
- > under Chapter 11 of the U.S. Bankruptcy Code.
- > Subject to court approval, Britain's Cable and Wireless plc has agreed to
- > purchase Exodus's data center assets. We cannot predict the effect this may
- > have on its ability to continue to provide reliable service.
- > We have engaged Equinix, which is located in the same geographical area,
- > to replace Exodus as our primary Internet hosting provider and intend to
- > complete this transition in the first quarter of 2002.

So how's the transition going?

- > Our infrastructure could prove unable to handle a larger volume of
- > customer transactions. Any failure to accommodate transaction growth
- > could impair customer satisfaction, lead to a loss of customers, impair
- > our ability to add customers or increase our costs,
- > all of which would harm our business.

With their inability to handle cutovers from emergencies, I don't see how that's making things scalable.

---

## **Ice-skating judging solution**

Ken Knowlton <KCKnowlton@aol.com>

*Tue, 19 Feb 2002 13:59:10 EST*

What a marvelous solution to the problem exposed by the Olympics ice-skate judging brouhaha: use computers and random numbers, and-- most important --

remove the process from public view!

[The algorithm reported: 14 judges, reporting anonymously, with the computer program randomly and without accountability throwing out a handful of votes. Sounds like we are once again back to the wonders of nonaudited electronic voting systems that have received so much discussion in RISKS, such as the following item. PGN]

---

## **⚡ Re: Miami-Dade OKs touchscreen voting (Price/PGN, [RISKS-21.90](#))**

Alan Brain <ab@softimp.com.au>  
*Fri, 15 Feb 2002 16:38:49 +1100*

The risks for vote-rigging on COTS systems [include]:

- a) Someone tweaks the BIOS of the voting machines.
- b) Someone tweaks the OS of the voting machines.
- c) Someone tweaks the applications code
- d) Someone tweaks the compiler.

a) Can best be dealt with via physical security only - have non-flashable BIOSes, and disallow unauthorised access.

The rest require both a publicly available Open Source codebase, and physical security to make sure that what you think is on the machine, actually is. And that the right OS has been installed, and the right compiler used.

Well, it's not a touchscreen system per se, but close enough.

Have a look at <http://www.elections.act.gov.au/EVACS.html>. The source code's available at <http://www.elections.act.gov.au/evacs.tar.gz>

Compile with a gcc compiler, run on FreeBSD or Linux.

Conversely, if the voting is being done with machines where the OS, Applications Sourcecode and Compiler aren't Open Source, then security is problematic.

---

## **✶ An unlocked system can be compromised quickly**

"Greg Searle" <greg\_searle@hotmail.com>

*Fri, 15 Feb 2002 12:41:06 -0500*

Audrie Krause's submission on non-profit's security brought up the problem of not locking a workstation when walking away from it. If you don't understand why locking your system is so important, try the following exercise. (Don't worry -- if you hit "Cancel" in the final step\*\* as instructed, it won't actually do anything. This sequence would be slightly different on Windows 95/98/ME boxes, which can't be effectively locked, anyway.)

On an unlocked system (preferably yours!):

Hit Windows Key-E to bring up an Explorer window.

Select the "C:" drive in the right pane (tab,down arrow, or click on it).

Hit Alt-Enter to bring up the Properties dialog for that drive.

Click on the "Sharing" tab.

Click "Share this Folder" if it is not selected.

Only if "Share this Folder" was already selected, click the "New Share"

button, enter a share name, and hit "OK".

\*\* Hit "Cancel" to dismiss the dialog safely. DON'T HIT OK.

Close the Explorer window.

If you had hit "Ok" instead of "Cancel" above, this sequence would give

EVERYBODY TOTAL ACCESS to the C: drive. This means that anyone on the local

net could read and write any file or directory on your drive, and you

wouldn't know it. A malicious person with physical access to the machine

only cares about being able to freely access your machine from the privacy

of another workstation. They don't care that everybody else has access, as

well.

So, how long did the exercise above take you? It would only take less than

10 seconds for an experienced Windows user, and there is no visible evidence

that the system was tampered with. How long does it take for you to walk to

the coffee machine and back? Lock your systems when you walk away. This

exact thing actually happened to an employee at the company I work for.

Eventually she realized that her system was wide open to the network.

Worse, some damage had been done by a remote user. They never found out who

did it.

If you're worried that I'm giving away some secret information, don't. This

can be accomplished in many ways, and the information is public knowledge.

This particular sequence would usually be selected as the

fastest way to get  
in, make the change, and get out. I'm just attempting to  
impress how  
quickly a Windows system can be compromised.

(If you really hit "Ok" instead of "Cancel", you will want to  
remove the new  
share, quickly.)

---

## **⚡ Dangerous characters**

"Mark Lomas" <mark.lomas@tmalomas.com>

*Fri, 15 Feb 2002 00:06:57 -0000*

Many of us are familiar with web sites that, because of  
inadequate checking  
of user-supplied data, are vulnerable to attack. Careful  
filtering of data  
can prevent such attacks.

Waitrose, a well-respected chain of UK shops, took this a little  
too far on  
their on-line shopping site. It appears that they decided that  
the humble  
apostrophe was too dangerous to appear in user input.

I noticed this because it changed the message I had asked to be  
sent with  
some flowers for my wife. As today is St Valentine's day, I  
imagine a large  
number of customers had their messages changed.

---

## **⚡ Computerized assistance with non-standard punctuation**

"David Piper" <dxp7949@lausd.k12.ca.us>

*Thu, 14 Feb 2002 08:33:11 -0800*

In [RISKS-21.91](#) Toby Gottfried notes potential problems with the name of Microsoft's new project ".Net" violating common rules of English sentence structure. Robert Marshall advises that Google may be stripping self-defined "extraneous" punctuation from email addresses.

I used to live on a street called "Oak Crest Way". One day my address was OCR scanned by some mailing list company and the "O" was resolved as a period. I then began to receive junk mail addressed to:

".Ak Crest Way"

Notice how the "intelligent" software automatically capitalized the "A". I received several pieces from different junk mailers as the address was resold. Then one day a new junk mail piece arrived addressed to:

"Ak Crest Way"

Another "intelligent" program had automatically stripped out the leading period. I don't have high hopes for ".Net".

David R. Piper, Administrative Analyst, Los Angeles Unified School District  
Maintenance&Operations, District I, 1500 E. 14th Street, Los Angeles, CA 90021

---

**✶ Re: Homograph problems (Kline, [RISKS 21.91](#))**

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

*Sun, 17 Feb 2002 17:12:24 +1100*

Merlyn Kline mentions homograph problems with lowercase L, uppercase I, and the number 1. I had the misfortune to encounter a net access program that gave me a randomly-generated password with three of these in it... and wouldn't allow font changes. With 27 possibilities to try, I was glad it didn't lock-out after three failed attempts.

Geoffrey Brent

---

## ✶ What's a buffer overrun problem?

"William P. N. Smith" <wpns@compusmiths.com>

*Wed, 13 Feb 2002 10:46:41 -0500*

Something about being doomed to repeat history:

> Software: Telnet Service in Microsoft Windows 2000; Telnet  
> Daemon in Microsoft Interix 2.2  
> <http://www.microsoft.com/technet/security/bulletin/MS02-004.asp>.

[...]

> The implementations [...] contain unchecked buffers in the  
> code that handles the processing of telnet protocol options.

and

> Software: Microsoft Windows 95, 98, 98SE, NT 4.0, NT 4.0  
Terminal  
> Server Edition, 2000, XP  
> <http://www.microsoft.com/technet/security/bulletin/MS02-006.asp>.

[...]

> A buffer overrun is present in all implementations [of SNMP].

It's nice that they are closing holes, but with all the Navy shipboard networks that are apparently running Windoze, 'overflow' is going to take on a brand new meaning. 8\*}

William Smith      wpns@compusmiths.com      N1JBJ@amsat.org  
ComputerSmiths Consulting, Inc.      www.compusmiths.com

---

## **⚡ Sorry, that number is now in service**

Gene Spafford <spaf@cerias.purdue.edu>  
*Mon, 18 Feb 2002 09:03:23 -0500*

Long ago, I configured the router for our center to reject packets coming from nonsensical addresses. These include packets coming from the outside with addresses of inside hosts, with the loopback address as source, and with any unassigned IP addresses. The latter were taken from the IANA list of "reserved" IP ranges.

Blocking these packets helps keep away packets employing address spoofing and DOS attacks with falsified "from" addresses. Needless to say, this is a desirable outcome!

Because our router config is complicated, it is something I try to avoid changing (or even looking at) unless something breaks. Usually, that is obvious -- we install something new, or add a new subnet, and things need to be adjusted.

About 3 months back, my email to a long-time friend started bouncing. Well, to be specific, it would sit in our queue and timeout -- it couldn't seem to get delivered to the destination. I didn't think much about it because hosts sometimes go down. Plus, her company was undergoing some expansion and moving offices. But the problem persisted. A mutual friend reported no such problems, which really seemed odd.

Then, I tried sending email from a separate account I have outside the university. It got through! But email to my account at CERIAS failed. How odd... Further investigation revealed that I could do a traceroute right up to her company's firewall, but no further. Meanwhile, the admin at her firm reported he could traceroute to our router, but no further. Really odd!

An inquiry to their ISP revealed no filter rules that blocked traffic. And I could reach their machine from other campus hosts. It must be our router.

It took me nearly a full day to find the offending line buried deep within the router config. This was complicated because I generate part of the config using a macro preprocessor (saves some of the tedium of typing the almost-same line over and over).

It appears that sometime in 2001, the 69.x.x.x IP range (plus others) went from "reserved" to "assigned". However, if there was some place this was announced, I never saw it (or it never registered to me).

Meanwhile, my  
router was happily blocking all the traffic from my friend's  
site.

There must be a moral to this story, but I am unsure what it  
might be. I  
can say that I am still blocking address ranges, but now I have  
a reminder  
in my mailer to check the assigned number list every 6 months.

---

**⚡ Re: Officer calls for refund of 'speeding' fines (Solomon, [R 21 91](#))**

Henry Baker <hbaker1@pipeline.com>  
*Fri, 15 Feb 2002 13:31:26 -0800*

This is a very old problem. Road & Track did an article 25+  
years ago about  
Italian drivers who would take their cars out on the Autostrada  
tollroad and  
keep and frame the stamped toll receipt which proved that they  
achieved 200  
kilometers per hour (or whatever) for a particular Autostrada  
segment.

I think that the Italian government got wise and started  
automatically  
printing out speeding tickets along with the toll receipts!

---

**⚡ Re: Social Security numbers on tax envelopes (Klein, [RISKS-21.91](#))**

"Robert Ellis Smith" <ellis84@ma.ultranet.com>  
*Thu, 14 Feb 2002 12:45:57 -0500*

Gee, a new federal law prohibits federal agencies from doing this - but it doesn't kick in until November 2004!, according to Privacy Journal's new Compilation of State and Federal Privacy Laws.

Robert Ellis Smith, Publisher, Privacy Journal, Providence RI  
privacyjournal@prodigy.net <http://www.privacyjournal.net>

---

## **✶ The Security Risks of Programs That Automatically Update**

Scott Schram <scott@schram.net>  
*Fri, 15 Feb 2002 09:31:47 -0600*

I've just completed an article addressing some risks of programs that update themselves:

Rather than a bona-fide update, the auto-update feature could be used to send programs with undesired features. The activity of these updaters would not be detected by firewall tools, as they are expected to be periodically checking for updates and downloading them. Further, the most careful reverse-engineering of the updater would not reveal anything unexpected.

<http://schram.net/articles/updaterisk.html>

Comments are welcome! Thanks,

Scott Schram <scott@schram.net> <http://schram.net>

---

## ✦ New Security Conference - GOVSEC, Call for Presentations

Jack Holleran <Holleran@severnapark.com>

Thu, 14 Feb 2002 00:22:20 -0500

[Jack is seeking participant ideas, not completed works,  
by 23 Feb. PGN]

As the program develops, information will be posted on  
<http://www.govsecinfo.com>

GOVSEC 2002 is the only conference dedicated to enterprise security for the government. GOVSEC offers two powerful conferences in one. GOVSEC will address physical security issues and information security issues.

If you have any questions on submitting a Call for Presentations for GOVSEC 2002, please contact Sharon Patterson, CMP, at [spatterson@ntpshow.com](mailto:spatterson@ntpshow.com) or call 703.941.5896.

GOVSEC is produced by National Trade Productions, Inc.  
313 S. Patrick Street, Alexandria, VA 22314. Phone 703.683.8500



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 21: Issue 93**

**Tuesday 5 March 2002**

## Contents

- [Malfunction shuts down computer-controlled amusement park ride](#)  
[Chuck Hardin](#)
- [A\\$ 22,000 in fines for missing car-toll transponder](#)  
[Peter Trei](#)
- [Air Transat emergency landing](#)  
[John Johnson](#)
- [Nick Petreley: Identity theft](#)  
[Anthony W. Youngman](#)
- [Metro: Time runs out for Domesday discs](#)  
[Chris Leeson](#)
- [RISKS to computers from society](#)  
[Arthur J. Byrnes](#)
- [Corporate Web sites leave cold steely feeling](#)  
[Dan Jacobson](#)
- [Tunneling too close to the person you're trying to protect: SafeWeb](#)  
[David Martin](#)
- [Privacy risk in Netscape 6](#)  
[Sim IJskes](#)
- [Electronic Voting in Ireland](#)  
[Peter Thornton](#)

- [Re: Miami-Dade OKs touchscreen voting](#)
    - [Les Barstow](#)
    - [Mark Nelson](#)
  - [Re: The homograph problem](#)
    - [Partha](#)
  - [Re: Dangerous Characters](#)
    - [Dick Botting](#)
    - [Darrell Fuhriman](#)
    - [Bill McGonigle](#)
  - [REVIEW: "Security Fundamentals for E-Commerce", Vesna Hassler](#)
    - [Rob Slade](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

## ⚡ Malfunction shuts down computer-controlled amusement park ride

Chuck Hardin <chardin@suchdamage.org>

Sat, 02 Mar 2002 08:57:38 -0600

[http://news.bbc.co.uk/hi/english/uk/england/newsid\\_1850000/1850592.stm](http://news.bbc.co.uk/hi/english/uk/england/newsid_1850000/1850592.stm)

It was a perfect day in the capital for viewing the skyline from the giant

London Eye. But a computer problem made the 450-ft-high structure rotate

too fast, and it was halted amid safety fears. Engineers have been

brought in to get the attraction, officially known as the British Airways

London Eye, up and running again.

This calls to mind Ben Morphett's narrative in [RISKS-21.50](#) about a carnival

ride which gave him a bad moment by displaying a blue screen of death just

before it began its (planned?) rapid descent. The difference is

that in his case, the computer was merely providing some graphical effects and was not apparently responsible for controlling the ride. Not so in this case.

Four hundred and fifty feet is a long way to fall, or to be hurled, due to an ill-considered RISK.

---

## **⚡ A\$ 22,000 in fines for missing car-toll transponder**

"Trei, Peter" <ptrei@rsasecurity.com>

*Tue, 26 Feb 2002 15:20:10 -0500*

A man used City Link more than 220 times without an e-tag, attracting at least \$22,000 in fines, because he did not know it had become a toll road, the Melbourne Magistrates Court was told yesterday. [...]  
<http://theage.com.au/articles/2002/02/26/1014704951335.html>

Some highways in Australia cannot be legally used without a radio tag. This poor soul hadn't updated his address with the DMV. The RISK lies in building systems which automatically rack up charges without limit, and no backup notification system. A big flashing sign saying 'E-Tag missing!' might have helped. Peter Trei

---

## **⚡ Air Transat emergency landing**

<john.johnson@dalsa.com>

*Mon, 4 Mar 2002 15:36:27 -0500*

I thought RISKS readers would be interested in a developing story in the news about a computer problem on the Canadian Air Transat flight that made an emergency landing in the Azores last summer. Apparently, as early reports describe, a "computer program" incorrectly reported a fuel leak as an "imbalance". To correct the "imbalance" the "computer program" diverted fuel from a good tank to the tank that was leaking thus both tanks were emptied. Inflight. The skill of the pilot and the availability of an island with an airport in the Atlantic Ocean averted a disaster.

Source: Canadian Press, \*Toronto Globe and Mail\*, \*Toronto Star\*, & other Canadian newspapers

---

## **✈ Nick Petreley: Identity theft**

"Anthony W. Youngman" <Anthony.Youngman@ECA-International.com>  
*Thu, 21 Feb 2002 13:05:11 -0000*

[http://www.computerworld.com/cwi/story/0,1199,NAV47-74\\_ST068446,00.html](http://www.computerworld.com/cwi/story/0,1199,NAV47-74_ST068446,00.html)

Nick Petreley's \*Computerworld\* column (18 Feb 2002) describes how some unknown person hijacked his phone account and made loads of long-distance calls "at his expense". The saga goes from bad to worse as poor security and company incompetence frustrates his attempts to stop the

fraud.

[After noticing the frequent calls to Germany, Nick canceled his calling card and switched his long-distance carrier. The person who had been piggybacking on his old card then managed to switch his new account back to the old carrier and make more calls. It turns out that person had created a Web account for him, so that he no longer received statements. The entire saga is a real horror story, and very well worth reading. Lots of lessons to be learned. PGN]

---

## 🔥 Metro: Time runs out for Domesday discs

"LEESON, Chris" <CHRIS.LEESON@london.sema.slb.com>

*Mon, 4 Mar 2002 09:51:50 -0000*

The BBC's 1986 Domesday Project (a time capsule containing sound, images, video and data defining life in Britain) is now unreadable. The data was stored on 12-inch video discs that were only readable by the BBC Micro, of which only a handful still exist. The time capsule contains "250,000 place names, 25,000 maps, 50,000 pictures, 3,000 data sets and 60 minutes of moving pictures.". The article notes that the original Domesday Book (compiled in 1086 for tax purposes) is still in "mint condition". [Source: London \*Metro\*, 01 Mar 2002]

Additional comments of my own:

The BBC Micro, along with the original Sinclair Computers, was

the computer that sparked off the "computer revolution" in the UK. The BBC Micro was especially popular in schools, whereas the Sinclair computers were more popular in the home.

To be fair, the 1986 Domesday Project was in the days before the really rapid changes in technology came into force - the BBC Micro was not a bad choice of platform then, especially when you consider that there were very few other choices available (50,000 pictures alone take up a lot of space).

Moral/Risk: If you are wanting long-term data storage, the format is just as important as the materials.

This is not a new problem - It has appeared in Risks before ([RISKS-21.56](#):

'NASA data from 1970s lost due to "forgotten" file format' for one...), but is worth keeping in mind. I still have an old Commodore 64/128 disk with my (very) old account details on it - not that I have a C64/128 any more. My permanent records, however, are the printouts.

PS: "Domed... We are all Doomed..."

---

## **✶ RISKS to computers from society**

"Arthur J. Byrnes" <arthur@ajb.com>

*Sat, 23 Feb 2002 20:53:21 -0500*

Reading the various articles about buffer overflow and WiFi

security  
problems, makes you think that Society has to worry about risks  
from  
computers.

Then I have two incidents in one week that remind me that  
computers are the  
ones at risk.

First a I get a misdirected plain-text e-mail from a major  
insurance company  
with login IDs, passwords, and usage instructions, (that seemed  
to come  
from one of those "Dummies" books). As much as my curiosity  
wanted to try  
them out, my ethics stopped me. A note to the company got an  
auto reply, no  
thanks, or inquiry about how/why I ended up with this seemingly  
important  
e-mail.

Then later in the week I added a new Web site to my Microsoft  
Central  
account. The welcome plain-text e-mail contained my login name  
and password,  
which is also my .Net login. They made clients sign up for .Net  
in order to  
continue using their service. (I'm glad I don't use it for  
anything else!)

Two major companies that should have known better, put Society's  
computers  
at Risk, with a practice that is unpardonable. Never send login  
IDs and  
passwords together...

Arthur J. Byrnes <http://www.ajb.com>

---

**✶ Corporate Web sites leave cold steely feeling**

Dan Jacobson <jidanni@deadspam.com>

28 Feb 2002 03:56:16 +0800

Now that I have traded my corporate life for "back to nature", every once in a while there is a long term bond from my past life or something that is about to expire, hence I must log on to some corporate site, wherein right off the bat:

Browser Upgrade

Thank you for visiting Jackson National Life Insurance Company's

Web site. We have noticed you are using an earlier version of null.

Also, aren't those little lock symbols supposed to lock when asking for SS#, passwd, etc.?

And don't you hate those Web sites that after filling in a long form, you are to pick which of the 50 states you live in... I get stuck here. I would have used the toll free phone # but it is not toll free for me.

OK, now turning to the AT&T Universal card site... Ah, AT&T, equal opportunity employer... OK, but still, cant use the Lynx browser... what if I was vision impaired? And, why after establishing that I am not spam, cannot I have an e-mail conversation with these corporate giants about compatibility issues with their Web sites without having to "login to send/receive secure e-mail"... takes half of my modem session.

<http://www.geocities.com/jidanni/> Taiwan(04)25854780

## **⚡ Tunneling too close to the person you're trying to protect: SafeWeb**

"David Martin" <dm@cs.bu.edu>

*Thu, 14 Feb 2002 16:50:52 -0500*

A tunnel is the prototypical example of a security mechanism that doesn't compose well: it creates an end-to-end connection that can bypass intermediate scrutiny. SafeWeb, the Web anonymizing service, fell into this trap by attaching the browser end of its tunnel too closely to the user and thereby bypassing meaningful browser protections. The result is that users of the service are at higher risk of some types of privacy attacks than those who refrain from using the service.

Note that SafeWeb's anonymizing service was shut down in December for business reasons. However, its technology was licensed to In-Q-Tel (the venture capital firm funded by the CIA) and PrivaSec LLC. PrivaSec is currently offering a public beta test of its service based on SafeWeb's technology at its Web site <http://www.privasec.com>. For simplicity, we'll pretend the system is still running at safeweb.com in the rest of this article.

First a quick SafeWeb overview: a SafeWeb user types in a URL. It goes to safeweb.com within an SSL connection; SafeWeb sanitizes the requested content and delivers it back to the browser. The origin server Web site

only sees a connection from safeweb.com, and eavesdroppers near the user only see an encrypted connection to safeweb.com On-screen, SafeWeb uses frames to separate the SafeWeb controls from the requested content. Let's call them the "control" and "content" frames.

Now let's meet the protections: (1) simultaneously open windows or frames can only communicate with each other if they're from the same domain, (2) scripts stop running when a new page is displayed, and (3) cookies are available only to the domain that set them.

The problem is that both of SafeWeb's frames are served from the same tunnel (<https://www.safeweb.com/>) even though their content comes from radically different sources: the trusted SafeWeb site on the one hand, and the untrusted third party site on the other. Since both frames come from the same domain, the Web browser exposes each Document Object Model to the other: protection #1 is gone.

Since the control frame is basically static, it's a great place for an attacker to tuck away any code that needs to persist throughout the browsing session -- like spyware. So protection #2 is gone too.

SafeWeb also wanted to support pseudonymous persistent cookies. Since the content frame is always associated with a single privacy domain, they aggregated all of the pseudonymous cookies from sites a user might visit through SafeWeb into one "master cookie" associated with the fixed domain safeweb.com. That way, the individual cookies all get stored on

the user's computer in a slightly different form, and SafeWeb doesn't have to maintain any persistent state on their servers (and users don't have to log in to SafeWeb, etc.). But this approach discards protection #3 as well.

To exploit these lost protections, an attacker has to take control of one of the frames: the content frame is the obvious choice. That turns out to be not too hard. SafeWeb *requires* that JavaScript be enabled in the browser. Recognizing the risk, SafeWeb tried to sanitize scripts delivered to the content frame, but they didn't go nearly far enough. The result? By choosing to use this privacy enhancing system, users become vulnerable to having their IP address revealed, *all* of their cookies stolen, and the remainder of their privacy-"enhanced" browsing session silently transmitted to an attacker in spite of the layer of SSL protection. This is not speculation; we have tested several effective exploits against the system.

Discarding protection mechanisms is only justified if those protections are replaced by something stronger, or by something more valuable to the end users. SafeWeb's system did keep its users' identities out of routinely gathered Web server logs. But the cost was increased vulnerability to targeted attacks, and it's hard to say whether the system's users would consider this a good tradeoff. There's no reason to think they would be aware of the tradeoff at all.

Adding to the weirdness, we are told that this privacy enhancing service was subjected to a "stringent" technological review by the CIA.

Details (24 pages, PDF) are available at <http://www.cs.bu.edu/techreports/pdf/2002-003-deanonymizing-safeweb.pdf>.

In response to our observations, SafeWeb points out that their own service is no longer in operation, that their new products didn't inherit these problems, that the system was effective at resisting passive attacks, and that the adversaries they had in mind wouldn't have been willing to use attacks such as ours for fear of bad publicity. They have also announced that they are developing a fix for their licensees, In-Q-Tel and PrivaSec.

David Martin -- dm@cs.bu.edu  
Andrew Schulman -- undoc@sonic.net

---

## ✶ Privacy risk in Netscape 6

Sim IJskes <sim@nyx.xs4all.nl>  
*Thu, 21 Feb 2002 21:05:43 +0100*

I just installed the Netscape browser version 6.2. I changed 'Internet search' options so that Netscape performed searches through Google instead of the Netscape search engine.

Some browsing in the files that were installed led me to this line:

action="[http://info.netscape.com/fwd/lksidus\\_gg/http://www.google.com/search](http://info.netscape.com/fwd/lksidus_gg/http://www.google.com/search)"

in a file "SBWeb\_02.src". It looked as if Google directed search requests are first sent to info.netscape.com. A quick look in the proxy server log on the server confirmed my suspicion.

I guess that Netscape allows you to search other search engines than their own, but still wants to know what you are searching....

P.S. a similar mechanism was also used in the 'SmartDownload manager' some years ago, as i seem to remember (maybe still is).

Sim IJskes, Leiderdorp, The Netherlands | sim@nyx.xs4all.nl

---

## ✶ Electronic Voting in Ireland

"Peter Thornton" <Peter.Thornton@emr-radio.ie>  
*Mon, 25 Feb 2002 14:48:22 -0000*

Further to recent contributions on electronic voting, this is from the

Web site of the Irish department of the environment:

<http://www.environ.ie/press/electvote02.html>

The "forthcoming general election" they refer to will be taking place in the next three months. I note that they will be using "an industry standard PC system". I presume that this means a Wintel box.

Green Light For Electronic Voting In Dublin North, Dublin West And Meath

Mr Noel Dempsey TD, Minister for the Environment and Local Government has announced today (19 February) that the constituencies of Dublin North, Dublin West and Meath have been chosen as the pilot constituencies for the introduction of electronic voting. "Subject to final testing of software, my intention is that the voters in Dublin North, Dublin West and Meath will be the first in the country to cast their ballots electronically. Thus, the forthcoming General Election should usher in a new age of efficiency in the voting process," said Minister Dempsey. "Electronic voting will dramatically speed up the counting process with results for the constituencies likely to be available within a half an hour of the final module, on which the cast votes are stored, being delivered to the counting centres."

The electronic voting system to be used has been developed by the Dutch/UK company, Nedap/Powervote. The Nedap/Powervote solution will provide a 'fullface' (large screen) machine which is successfully used in the Netherlands and in the German cities of Cologne and Dusseldorf. Election preparation will be run from an industry-standard PC system and the completion of the count will also be carried out on a standard PC and programming unit.

In the run up to the introduction of electronic voting, there will be an intensive public information campaign in the constituencies concerned to ensure that all voters will be familiar with the new method of voting.

Peter Thornton, EMR Radio & Telemetry, Unit 11 Dunboyne Business Park  
Dunboyne Co. Meath Tel: +353-1-8013161

---

**Re: Miami-Dade OKs touchscreen voting (Price/PGN, [RISKS-21.90](#))**

Les Barstow <lbarstow@vr1.com>  
*Thu, 21 Feb 2002 07:03:28 -0700*

With physical access to voting machines and/or the software used to control them, the only sure way to provide security is a paper record.

Especially with OpenSource software, it becomes possible to recompile (and hence alter) any electronic-only record. Closed Source software isn't any better - it lacks public accountability and scrutiny. Someone could always create a new ROM, OS, or software image if given sufficient knowledge, bypassing any security system that has been put in place.

So: Print an OCR paper record when the voter finishes his vote. He gets to check the paper copy and put it in a standard secured voting box. The best parts are:

(a) Since it's printed on demand, only the voter's candidate appears on the printout - the voter sees only who or what he voted for, or that he made no vote, and can easily check the paper before

dropping it in the box.

(b) Using OCR, independent auditing becomes easy. The auditor needs little in the way of custom hardware or software to do the job; they only need to tweak their OCR readers. Auditors could be chosen by mutual agreement of the candidates after the vote is completed (and only if a candidate determines he wants to have a recount), removing any temptation to bribe the auditing firm.

Les Barstow, System Administrator, VR1, Inc.

<http://www.vr1.com> lbarstow@vr1.com

[We've been talking about such schemes before here. See Rebecca Mercuri's

PhD thesis for a detailed analysis:

<http://www.notablessoftware.com/~evote>

noted in [RISKS-21.10,13,14,61](#). PGN]

---

## ✶ Re: Miami-Dade OKs touchscreen voting (Brain, [RISKS-21.92](#))

Mark Nelson <mcnel1@h\_o\_t\_m\_a\_i\_l\_.c\_o\_m>

*Fri, 22 Feb 2002 15:56:57 -0500*

> The risks for vote-rigging on COTS systems [include]:

e) Someone tweaks the compiler of the compiler of the compiler of the...

See Ken Thompson's "Reflections on Trusting Trust"

<http://www.acm.org/classics/sep95/>

## **⚡ Re: The homograph problem ([RISKS-21.91](#) and 92)**

Partha <algolog@hd1.vsnl.net.in>

Thu, 28 Feb 2002 19:16:12 +0530

I am a victim of one such problem. Our Indian bureaucrats in the Govt.

owned ISP called VSNL decided to create domain names using a mixture of

alphas and Arabic numerals. Resultant: I have an e-mail address containing a

"one". It is impossible to make out the "one" from "lower case L", and as

result of which I lose many many e-mails destined for me. I have mitigated

the problem to a certain extent, by adding a descriptive note in my

signature box, but it is impossible to print such things on my visiting

cards. Notice that there is also a "lower case L" in the second field of my

domain name "v-s-n-L". We (Indians) are perhaps the only ones in the world

to have such confusing combinations of alphas and numerals in their domain

names.

When will we ever learn?

PS: VSNL has now been "privatised". They changed the owners but they

kept the brilliant employees who created this mad domain name.

Dr. S. Parthasarathy, Algologic Research & Solutions, 78

Sancharpuri Colony,

Bowenpally, Secunderabad 500 011 - INDIA Phone: + 91 - 40 - 775 1650

## **⚡ Re: Dangerous Characters (Lomas, [RISKS-21.92](#))**

Dick Botting <rbotting@csusb.edu>

*Thu, 21 Feb 2002 13:41:31 -0800*

This looks like the "sanitization" procedures for user supplied data that is recommended for the Perl language. Perl is used by many Webmeisters.

Typically, it has to call other programs and uses a "shell escape" to do so.

On UNIX boxes it does this in such a way that the shell interprets the passed data as a command. An apostrophe is a string delimiter and so a stray blip can play havoc with string data... A smart user can easily make the server execute any command. Hence User data is sanitized by removing certain characters.

Another solution is to avoid Perl. Scripts written in Bourne/Korn/Born Again SHell do not have this problem. Care is still needed, but the removal of the usual suspect characters is not necessary.

---

## **⚡ Re: Dangerous characters (Lomas, [RISKS-21.92](#))**

Darrell Fuhriman <darrell@grumblesmurf.net>

*21 Feb 2002 13:49:09 -0800*

I regularly have perfectly valid e-mail addresses rejected by Web forms because they contain a '+' sign. Most Web sites seem to assume that anything

not in the set [A-Za-z1-9\_-] is invalid, even though the valid set defined in RFC 2822 is much larger than that.

I wonder what's going to happen when, inevitably, e-mail addresses are allowed to be in Unicode. I fully suspect that we'll suddenly find a large portion of the population unable to use their nifty new language appropriate addresses.

---

## ⚡ Re: Dangerous characters (Lomas, [RISKS-21.92](#))

Bill McGonigle <mcgonigle@medicalmedia.com>

*Thu, 21 Feb 2002 11:46:48 -0500*

Probably Waitrose is storing their orders in a SQL database. In most SQL statements, apostrophes need to be escaped, typically as '' (that's two single quotes). I've met so-called Web-site programmers to whom the notion of an escape character suggests something out of a prison-break movie. Often they notice a problem, with the database of course, when trying to store text with an apostrophe, so they put some 'error checking' code in to prevent those errors.

---

## ⚡ REVIEW: "Security Fundamentals for E-Commerce", Vesna Hassler

Rob Slade <rslade@sprint.ca>

Mon, 4 Mar 2002 07:44:27 -0800

BKSCFUEC.RVW 20020108

"Security Fundamentals for E-Commerce", Vesna Hassler, 2001,  
1-58053-108-3, U\$83.00

%A Vesna Hassler hassler@infosys.tuwien.ac.at

%C 685 Canton St., Norwood, MA 02062

%D 2001

%G 1-58053-108-3

%I Artech House/Horizon

%O U\$83.00 800-225-9977 fax: 617-769-6334 artech@artech-house.  
com

%P 409 p.

%T "Security Fundamentals for E-Commerce"

"The purpose of this book is to give an in-depth overview of all  
the basic  
security problems and solutions that can be relevant for an e-  
commerce  
application." I'm sorry, but "in-depth overview" sounds a bit  
like "jumbo  
shrimp": it's an oxymoron. And "all the basic security problems  
and  
solutions that can be relevant for an e-commerce application"  
covers a lot  
of ground. (Which is, I suppose, why this text has twenty two  
chapters.)

Part one explains the basics of information security. Chapter  
one defines  
some of the basic jargon, but misses a number of the important  
fundamental  
terms. For example, the relationship between threats,  
vulnerabilities and  
exploits is fairly basic to security and risk analysis, and yet  
all security  
problems seem to be lumped together as threats. The examination  
of security  
mechanisms, in chapter two, is limited to cryptography. Key  
management is  
restricted to X.509 certificates and Diffie-Hellman in chapter

three.

Part two looks specifically at security of electronic payment systems.

Chapter four briefly lists a wide variety of payment systems. A terse set

of payment security problems is given in chapter five, while some seemingly

random cryptographic solutions are given in six. A little bit of math for

functions directed at electronic cash and cheques is presented in chapters

seven and eight, respectively. Chapter nine describes the Internet Open

Trading Protocol.

Part three deals with communications security. Chapter ten is a general

look at networking. Chapters eleven to fourteen examine different systems

for security at different layers, but the depth of coverage is very

inconsistent: extremely terse in some cases, with many gaps, and yet delving

into minute detail in others.

Part four examines Web security. Chapter fifteen details the HyperText

Transfer Protocol (HTTP), which is good, since few texts bother to do.

Random topics related to Web servers make up chapter sixteen. Web client

security topics are dealt with somewhat better in chapter seventeen,

although cookies aren't given any significant discussion.

Active content

does get its own chapter: eighteen concentrates almost exclusively on Java.

Chapter nineteen contains miscellaneous topics.

Part five covers some special issues for mobile or agent computing. Agent

technology is described in chapter twenty, some cellular phone

topics are reviewed in twenty one, and smart card security is discussed in twenty two.

Well, overview it is. The book does cover a variety of topics, although there are a great many gaps and holes. However, "in-depth" can't be supported, except in a very few cases. There are some topics that are discussed in excruciating detail, but they are definitely in the minority.

As a college text this undoubtedly has its uses, but professionals or businesspeople will find the inconsistent coverage problematic.

copyright Robert M. Slade, 2002 BKSCFUEC.RVW 20020108  
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 21: Issue 94

Monday 11 March 2002

## Contents

- [Runaway remote-controlled coal train](#)  
[PGN-ed from Dan Swinehart](#)
- [LED lights can reveal computer data](#)  
[NewsScan](#)
- [Yet another case of a program changing your input](#)  
[Vassili Prevelakis](#)
- [Loosing It's Grammer Skill's](#)  
[Greg Searle](#)
- [.org.au, .gov.au, .edu.au domain hijacking through lax security](#)  
[Grant Bayley](#)
- [Amendment to add life prison terms for reckless hacking](#)  
[Len Lattanzi](#)
- [The computing battlefield](#)  
[Jon P](#)
- [Military palmtop will direct air strikes using WinCE](#)  
[David Wagner](#)
- [The next step in malicious spam](#)  
[Joe Faber](#)
- [The RISK of ignoring permission letters](#)  
[Timothy Knox](#)

- [Re: Air Transat Incident, Aug 24, 2001](#)  
[Peter B. Ladkin](#)
  - [Re: Malfunction shuts down ... amusement park ride](#)  
[Stanislav Meduna](#)
  - [Re: PayPal's tenuous situation](#)  
[Max](#)
  - [Info on RISKS \(comp.risks\)](#)
- 

## ✶ Runaway remote-controlled coal train

"Peter G. Neumann" <neumann@csl.sri.com>  
*Mon, 11 Mar 2002 11:57:53 PST*

Operating with a less-than-a-year-old remote-controlled system, a runaway train plowed through NIPSCO's Michigan City Generating Station on the morning of 7 Mar 2002, hitting another locomotive before the second locomotive's engineer narrowly jumped to safety. The unmanned eastbound diesel-electric engine, known as Big Blue, was pushing six coal cars when it approached the coal drop-off area at about 30 m.p.h. at 7:15 a.m. However, the train (in excess of 1.5 million pounds, including the coal) did not respond to radio controls and smashed through the enclosed thaw shed and coal rotary dumper, before smashing into the other train, Old No. 12. (Big Blue should have been going only about 1 mph for the last 100 yards entering the dumper.) The impact sent the other train through a fence, uprooted a bumper post, and ripped up track. A spokesman blamed it on a switch malfunction. But the system was supposedly designed so that if

the remote-controlled engine receives no signal, its brakes should automatically engage. Employees reportedly said that the system was not designed for the engines currently in use. Two other accidents occurred in the past month. Also noted was what sounds like a serious lack of receptivity from NIPSCO in responding to safety complaints from the workers' union over the past four or five years. [Source: No injuries in power station crash, by Jeff Tucker, \*The News Dispatch\* (thenewsd Dispatch.com), 8 Mar 2002, PGN-ed, contributed to RISKS by Dan Swinehart.]

---

## ✶ LED lights can reveal computer data

"NewsScan" <newsscan@newsscan.com>

*Thu, 07 Mar 2002 09:19:26 -0700*

Scientists in the U.S. and the U.K. have found a way to remotely eavesdrop on a computer by monitoring the flashes of LED lights on electronic devices. Optical signals from the light-emitting diode lights found in computer modems and keyboards can be captured with a telescope and processed to reveal all the data passing through the device, says Joe Loughry, a computer programmer at Lockheed Martin. "It requires little apparatus, can be done at a considerable distance, and is completely undetectable. In effect, LED indicators act as little free-space optical data transmitters, like fiber optics without the fiber." Loughry says the most

vulnerable

devices are equipment used in low-speed, long-distance networks, such as

ATMs (automatic teller machines). Corporate LANs and home Internet

connections are generally not susceptible to the spying technique. Loughry

says his interest in LEDs dates back to his days in graduate school: "I was

working very late one night and waiting for a long file transfer to complete

and I was just staring at these lights on the front of the modem and started

to wonder if there was anything there." Loughry recommends locating

equipment away from windows, putting black tape over the LEDs or deactivating when not in use. (Reuters 7 Mar 2002, NewsScan Daily, 7 Mar 2002)

["http://story.news.yahoo.com/news?tmpl=story&cid=581&u=/nm/20020307/tc\\_nm/tech\\_snooping\\_dc\\_1"](http://story.news.yahoo.com/news?tmpl=story&cid=581&u=/nm/20020307/tc_nm/tech_snooping_dc_1)

<http://story.news.yahoo.com/news>

?tmpl=story&cid=581&u=/nm/20020307/tc\_nm/tech\_snooping\_dc\_1

---

## **✶ Yet another case of a program changing your input**

<vassilip@dsl.cis.upenn.edu>

*Sun, 10 Mar 2002 07:18:39 -0500 (EST)*

I was entering grades in an Excel spreadsheet and realized that although in

my notes I had a mix of A's and A-'s, the spreadsheet had changed all the A

grades to A-'s. Why?

I was entering grades looking at my notes and not the screen. So I typed A-

followed by ENTER, then A at which point Excel suggested A- as a possible

input. Without looking I pressed ENTER, thus entering A- instead of A.

This only works if the longer input precedes the shorter in the original list (i.e., the list you are typing from), since if there is ambiguity about the suggestion, Excel shuts up.

Next time I think I will use vi.

---

## **Loosing It's Grammer Skill's**

"Greg Searle" <greg\_searle@hotmail.com>

*Wed, 6 Mar 2002 13:17:20 -0500*

It seems that with the advent of cheap publishing technology such as the Web, e-mail, and the laser printer, anybody can publish an electronic article or print up hundreds of signs. This has created an accelerating downhill trend as to the quality of the print material that we are exposed to every day. Back in the old days when only professionals with expensive equipment could create signs, flyers, and the like, these materials were proofread by skilled experts before they were published. The occasional error in grammar or spelling was very rare. Now, with the average Joe being able to mass-create signage and flyers easily, there is no professional between Joe and the printer to protect us from Joe's bad grammar.

For example, a local taxi company has printed bumper stickers and signs that boldly state on every single taxi, "Driver's Wanted". Tell me,

what of such  
a driver do they want? Signalling skills? Sure, I know what  
they really  
mean, but this error is now so common as to be annoying. How  
often do you  
see something like, "loose those extra pounds" exclaimed from a  
cheap ad?  
I'd rather get rid of them altogether, thank you, instead  
letting those  
pounds run loose.

Many businesses lose potential customers before they even make  
them, because  
of stupid mistakes in their literature, and they often wonder  
why. Who  
wants to do business with a company that can't even get its  
documents right?  
To a business looking to hire out some work, sloppy errors on a  
potential  
contractor's literature are telltale signs that something else  
may be wrong  
at that business, and are a cue to look elsewhere.

Lax proofreading standards are becoming more common as  
corporations look  
toward the bottom line, and want to save a buck. Why hire an  
expensive  
publishing company to compile and print your manuals, when an  
internal  
employee can hand a disc to Copy Cop and turn out a few hundred  
nicely-bound  
copies? The end result is a lot of lower-quality  
documentation. I took a  
Java class recently, and the training agency's course documents  
were riddled  
with stupid errors. Some of these were even in the code  
examples. This is  
supposed to be a professional training agency. They need to  
train their  
documentation department on higher proofreading standards.

English is defined by its common usage over an extended period  
of time. Are

we doomed to accept bad grammar as the official standard? Sure, computers make publishing easier, but the integrity of our language is at risk.

---

## **🔥 .org.au, .gov.au, .edu.au domain hijacking through lax security**

Grant Bayley <gbayley@ausmac.net>

*Wed, 6 Mar 2002 22:45:52 +1100 (EST)*

A colleague of mine recently came across a disturbing lack of security in the recently set up AUDA/AUNIC Registration Services for all .org.au, .gov.au and .edu.au domain names.

To cut to the chase on what the problem is, as of 6th March, 2002, you could enter any .org.au, .edu.au or .gov.au domain, any NIC handle and any password, and the system would accept, redelegate and makes the changes live in an average of less than 10 minutes. It didn't even check the password at all.

No doubt the hole will have been plugged by the time this makes it into RISKS, and no doubt any genuinely radical and unauthorised changes will have been reversed, but the scope of this vulnerability should be obvious.

Feel like picking up all the Web traffic and e-mail for your favourite federal law enforcement or communications intelligence agency for maybe 12 hours? (afp.gov.au or dsd.gov.au)? Perhaps an entire state? (nsw.gov.au)

Scary. Very scary.

Yet another indictment of the flimsy DNS system on which we all rely.

---

## ✚ Amendment to add life prison terms for reckless hacking

Len Lattanzi <Len.Lattanzi@Migration.com>

*Wed, 6 Mar 2002 11:27:15 -0800*

>From SANS NewsBites Vol. 4 Num. 10, 27 Feb 2002  
Life Sentences Proposed for Reckless Hacking

A US House subcommittee voted unanimously to propose lifetime jail sentences

for hackers who knowingly attempt "to cause death or serious bodily injury"

through electronic means.

<http://www.wired.com/news/politics/0,1283,50708,00.html>

What should the punishment be for recklessly allowing remote access to critical machinery and data?

---

## ✚ The computing battlefield

"Jon P" <cjmail@charter.net>

*Wed, 06 Mar 2002 17:59:25 -0500*

On 5 Mar 2002, National Public Radio aired a segment talking about the effort to put technology onto the battlefield.

"Anthony Brooks of the WBUR program "Inside Out Documentaries," reports on efforts by the United States Army to create a lighter more streamlined fighting force. Soldiers at Fort Lewis in the state of Washington are developing an "Interim Brigade Combat Force," which would have the agility of light infantry, combined with some of the punch of heavy armor. The idea is to make the force deployable anywhere in the world within 96 hours."

<http://search.npr.org/cf/cmn/cmnpd01fm.cfm?PrgDate=03%2F05%2F2002&PrgID=2>

The most chilling quote comes from an executive officer talking about how battlefield data is distributed and presented to soldiers in Humvees and armored vehicles: "We use nothing but Windows NT systems, that are hardened, to provide HTML products, which are nothing but homepage products, to disseminate the information via regular Internet protocols." (At 5:05 into the audio segment at <http://www.npr.org/ramfiles/atc/20020305.atc.02.ram>)

Gives new meaning to "Blue Screen of Death".

The full documentary report is available at <http://insideout.wbur.org/documentaries/reshapingmilitary/>

---

## ✶ Military palmtop will direct air strikes using WinCE

David Wagner <daw@cs.berkeley.edu>  
*Sun, 10 Mar 2002 00:05:00 -0800 (PST)*

\*New Scientist\* is reporting that the US military is planning to deploy palmtops for ground troops to use in transmitting targeting information for air strikes and the like. The application software will be running on top of Windows CE.

<http://www.newscientist.com/news/news.jsp?id=ns99992005>

---

## **✶ The next step in malicious spam (From Dave Farber's IP)**

Joe Faber <joefaber@alumni.princeton.edu>

*Sat, 09 Mar 2002 11:28:46*

I'm used to ignoring spam, but this morning I woke up to find that I received no fewer than three 160K+ .exe attachments in my inbox purporting to be from Microsoft. They were from the "Microsoft Corporation Security Center" and used "Internet Security Update" as their subject heading. The e-mail explains that the attached patch is the "5 Mar 2002 Cumulative Patch that eliminates all MS Outlook/Express as well as six new vulnerabilities" [sic]. It goes on to list some of the specific vulnerabilities and system requirements. They even provide a link to a Microsoft security Web site (where I couldn't find any mention of the patch).

Aside from the issue of mailing 3 copies of a 160K attachment, I can't begin to think of the trouble this might cause with the number of people running

Windows who would just think that this is benevolent Microsoft looking out for them and would promptly open the attachment. I'm no spam hunter, but I'm keeping the e-mails around should anyone want to see the header information.

For IP archives see:

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

[Bogosity alert! This kind of seemingly helpful message could easily be used to do enormous damage. Although some of the alleged vulnerabilities are legitimate, the message itself is indeed a hoax, as noted subsequently in various media -- including Dave Farber's IP, to which Ari Ollikainen contributed an article by Robert Vamosi, Gibe worm poses as a Microsoft update, ZDNet Reviews & Solutions, 6 Mar 2002. BEWARE! Always book a gift (Trojan) horse in the south. PGN]

---

## **✶ The RISK of ignoring permission letters**

Timothy Knox <tdk-freshmeat@thelbane.com>

*Sun, 10 Mar 2002 01:53:14 -0600*

I received the following e-mail recently. The subject certainly sounded encouraging: We request your permission (presumably to start sending me spam). Great, thought I, I can just ignore this, and they will go away. However, when I got to the last sentence of the main paragraph, I found that their idea of requesting permission differs from mine. It

reads:

If you do not wish to have HelloDirect.com contact you via e-mail, please click the link below and your name will be deleted from our e-mailing lists immediately.

This is NOT requesting permission. This is warning you that by NOT responding, you are implicitly consenting to them sending you spam. With UCITA, this might even become legally acceptable (like click-wrap licenses).

Finally, note how they try to play it cool in the last paragraph, talking about how I 'requested' to be notified of special offers. This is an outright lie. The e-mail address they sent to was only ever given to one Web site, which is a company that does order fulfillment for some other software companies. I did NOT give that company permission to send me ANY special offers (I always decline), so this is a lie. I don't know if the software fulfillment folks sold my address, or if they had their database illegally copied, or if this address was harvested years ago (it has been inactive for that long) and just now used.

- ----- Begin Forwarded Message -----

Subject: Hello Direct requests your permission.  
Date Sent: Friday, 8 March 2002 10.09  
From: Hello Direct <welcome@MT.DIRECTQLICK.COM>  
To: tdk+dr@VUSHTA.COM

For over 14 years, Hello Direct has been recognized and respected as the leading resource for telecom products, solutions and information. HelloDirect.com is seeking your permission to send you up-to-date

information on current industry news, cutting edge telecom products and services, special offers and product reviews via its electronic newsletter, The Newswire. All of this valuable information delivered efficiently and electronically, to your e-mail inbox!!! If you do not wish to have HelloDirect.com contact you via e-mail, please click the link below and your name will be deleted from our e-mailing lists immediately.

<http://mt.directclick.com/u/?e=tdk+dr@vushta.com&pn=4002152103-C>

Sincerely,

Your friends at HelloDirect.com

\*\*\*Hello Direct respects your privacy. This message was delivered to you because you requested previously from another website to be notified of special offers from preferred partners like Hello Direct.

- ----- End Forwarded Message -----

---

**✉ Re: Air Transat Incident, Aug 24, 2001 (Johnson, [RISKS-21.93](#))**

"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>  
*Wed, 06 Mar 2002 11:05:44 +0100*

Whatever the status of the recent press commentary, John Johnson's brief account of the Air Transat incident [[RISKS-21.93](#)] is misleading in various respects, and I think it appropriate to set the record straighter.

Johnson says:

Apparently, [...] a "computer program" incorrectly reported a fuel leak as an "imbalance". To correct the "imbalance" the "computer program" diverted fuel from a good tank to the tank that was leaking thus both tanks were emptied.

First, the "imbalance" report was not "incorrect". A fuel leak in the main fuel tanks, in the engines, or in between, on this model aircraft can lead to a fuel imbalance warning. In circumstances such as this, a fuel imbalance warning can be the first sign of a fuel problem. That a fuel imbalance warning can be sign of a leak is specifically noted in the relevant section of the operating handbook. Section 2.09, "Abnormal Procedures", under "Fuel Imbalance" says, first "Caution: Do not apply this procedure if a fuel leak is suspected. Refer to FUEL LEAK procedures."

Second, digital avionics systems are not just "computer programs". They have many independent, dedicated programmable digital components. There are over ten interconnected digital systems on this aircraft which deal with the fuel, most of which are duplicated for redundancy. These systems contain programmed digital hardware.

Third, the systems involved in reporting a fuel imbalance are not identical with the systems involved in transferring fuel, although the major digital component, the Fuel Control and Monitoring System (FCMS), is involved in both. The FCMS is not a "computer program". It is two dedicated digital computers.

Fourth, fuel transfer between imbalanced tanks has been de rigeur in heavy aircraft for a half century, and automated in new designs for a quarter century now. The automation mostly saves pilots a lot of work and worry.

Fifth, the leak was not in the wing tank, but on the engine itself.

All of this information has been publicly or semi-publically available since the incident over six months ago.

Some more background.

The A330 is a twin-engined aircraft. Its main fuel tanks are in the wings, as on most aircraft. Engines burn fuel at differential rates simply because of individual differences. Such differential fuel burn means that there is more fuel on one side of the aircraft than the other after a while, which unbalances the aircraft. It is inefficient to correct this by aerodynamic control inputs; the standard procedure in large aircraft for the last half-century has been to transfer fuel between tanks to regain balance. Since the late 1970's, new aircraft have been designed to perform such transfers automatically or semi-automatically, and such aircraft have been in service since the early 1980's. On the A330, this control is performed by the Fuel Control and Monitoring System (FCMS).

The fuel leak was on the engine, upstream of the control and monitoring of the fuel burn. On a non-leaky system, integrating the fuel

burn since engine start ("total fuel burn"), and adding this quantity to the measured fuel in the tank ("fuel on board"), one should obtain the same figure as measured in the tanks at engine start ("ramp fuel"). All these quantities are available continuously to pilots of all transoceanic aircraft, and it has been good practice since transoceanic flying began to perform this standard check. On earlier generation aircraft, this was the main method of detecting a fuel leak.

The fuel leak was caused by a break in a fuel supply line on the engine, itself caused by chafing of the line, which in turn was enabled by improper installation of the engine. Why the engine had been improperly installed is a non-trivial matter with no apparent computer involvement.

The major question is why the pilots did not detect the fuel leak earlier than they did. Another question is as follows. Suppose the pilots had discovered the fuel leak at the earliest possible moment; suppose, further, that it had occurred at the most inopportune moment (at their furthest point from suitable landing, which was allowed to have been as much as two hours flying time away). Would the information available to the pilots have enabled them, even in theory, to attain a suitable landing site anyway without running out of fuel? You could shut down an engine and isolate a leaking tank, maybe even transfer fuel away from a leak, but most pilots are reluctant, for good reason, to shut down a working

engine at night over ocean, especially when they do not possess complete information about the situation (in-flight real-time analysis of such a problem is notoriously difficult and unreliable).

Concerning the first question, in September 2001, shortly after the incident, I saw two ways in which presentation of information made available to the pilots in such a case could be improved, and presented these ideas to colleagues, the manufacturer, and the Bluecoat 2001 conference. However, information available already in October showed that the features that concerned me played either no role, or at most a very minor role, in the incident. I should note that the fuel system automation makes available to pilots (and investigators) much more, and more accurate, information about the fuel state of the aircraft than is available on aircraft with lower levels of automation.

The second question concerns the practice of flying over water significant time away from suitable landing. So-called Extended Range Operations, or ETOPS, permission is granted to airlines for specific aircraft and crew, depending on the demonstrated reliability of equipment, personnel and maintenance. The incident aircraft was operating under "120-min" ETOPS, allowing it to fly up to 120 minutes away from a suitable landing site. The maintenance snafu caused Air Transat's ETOPS permissions to be prophylactically reduced to 60 minutes. The incident itself caused some to question the very basis of ETOPS, not just its assessment, along

the lines  
which I indicated above. After an initial flurry of worry, the  
issue has all  
but disappeared from the aviation technical press. However, it  
is still  
unclear to me whether it can be satisfactorily answered.

Finally, whatever their performance during the earlier phases of  
the  
incident, the crew glided their aircraft, without engines, at  
night,  
some 85 nautical miles (98 statute miles, 156 km) to an  
essentially  
perfect "dead stick" landing on an aerodrome they had never seen  
before,  
a US military base. It was the world's first dead-stick landing  
of a  
fly-by-wire aircraft, and a significant achievement.

Besides the passengers and their family, safety engineers also  
have a  
lot to thank the crew for. Had the aircraft and crew been lost,  
either  
in the ocean or on a landing attempt, almost all the information  
needed  
to reconstruct this highly significant incident and learn from  
it would  
also have been irretrievably lost.

ETOPS or no ETOPS, running out of thrust on a modern airliner is  
just  
not supposed to happen. The lessons to be learned from this  
incident  
are incomparably rich, and in many ways unique. Thank heavens,  
and  
skillful pilots, that no one was hurt.

Peter B. Ladkin Faculty of Technology, University of Bielefeld,  
Germany.

## **✶ Re: Malfunction shuts down ... amusement park ride ([RISKS-21.93](#))**

Stanislav Meduna <stano@meduna.org>

Wed, 6 Mar 2002 21:13:01 +0100 (CET)

I work in the area of process control systems. The systems capable of BSOD (blue screen of death) are normally *\*not\** used to control safety critical parts of a system. These functions are usually implemented in the programmable logic controllers, which are hard-realtime systems with much less ways to crash. The traditional operating systems are used for the higher level controlling, data storage and human-machine interface.

Software-based PLCs using e.g. NT (often with some realtime extensions) as a underlying system do exist, but I doubt that they are used where safety of humans is at risk. Nobody with a sane mind would risk that, regardless of the claims of the vendors of these extensions that a realtime task continues to run or at least performs a clean shutdown in the case of BSOD (but can be technically completely messed up due to a runaway third-party driver).

The article doesn't mention how much faster the wheel was turning. My speculation is that maybe the controlling computer did indeed instruct the wheel to turn too fast, but then a safety task in the PLC kicked in and halted the machine. This is how these things are supposed to work - the event was probably not really a "safety scare", as the BBC titled it.

Stanislav Meduna

---

## **✦ Re: PayPal's tenuous situation (Jonas, [RISKS-21.92](#))**

<max7531@earthlink.net>

*Thu, 21 Feb 2002 14:14:16 +0000*

After using PayPal to buy something, I learned something. I recently made a direct purchase from a web site through PayPal. After it became clear that the transaction would not take place, I issued a complaint through PayPal's complaint service. Not being satisfied at the short explanation of the complaint process, I decided to give them a call to see where I stood. After much cajoling, the operator told me that the person I transferred money to had had her account frozen due to a fraud investigation! Of course, PayPal never prevented her account from continuing to receive money after it had been frozen. When questioned further, the operator said that it was PayPal's policy to allow frozen accounts to continue to receive funds so they could continue to payoff claimants! It seems that PayPal has a fundamental flaw in the way it "protects" users. With normal credit cards, the credit card company must guarantee the transaction to the merchant, since he takes a risk by accepting a flimsy piece of plastic instead of cash for his valuable merchandise. With PayPal, the opposite should be true. They

need to protect the buyer, since the money is paid before she receives the goods. I can see how millions of dollars in fraud could be committed by exploiting this flaw (as long as PayPal is willing to reimburse complaint issuers. :)I'm still waiting on resolution, but I have no fear. Since I made the payment with an actual credit card, I plan on challenging the purchase through them if PayPal's response is unsatisfactory. Must have been something I read on RISKS about layered 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 21: Issue 95**

**Tuesday 12 March 2002**

## Contents

- [ATTBI / Eudora / SSL](#)  
[Jock Gill via Dave Farber](#)
- ['Phantom Menace' typing is just a Microsoft speech feature](#)  
[Dale Hawkins](#)
- [Re: Yet another case of a program changing your input](#)  
[Gene Wirchenko](#)
- [Re: Air Force seeks better security from Microsoft](#)  
[Tom Poe](#)  
[Jei](#)
- [Disclaimers](#)  
[Michael Bacon](#)
- [Re: Loosing It's Grammer Skill's](#)  
[Michael Bacon](#)  
[Klaus Brunnstein](#)  
[Mike Albaugh](#)  
[Merlyn Kline](#)  
[Dave Williams](#)
- [Re: The RISK of ignoring permission letters](#)  
[Rob Slade](#)  
[Greg Searle](#)  
[George C. Kaplan](#)

[Michael Bacon](#)

● [Re: Welland Canal Bridge runs into ship](#)

[Dave Gillett](#)

● [Re: LED lights can reveal computer data](#)

[Nick Simicich](#)

[Peter B.](#)

● [REVIEW: "Incident Response", Kevin Mandia/Chris Procise](#)

[Rob Slade](#)

● [Info on RISKS \(comp.risks\)](#)

---

## ATTBI / Eudora / SSL

Jock Gill <jock@jockgill.com>

*Tue, 12 Mar 2002 10:03:52 -0500*

[From Dave Farber's IP list.]

Eudora users who are ATTBI customers might want to know this.

As Eudora users will know, ATTBI Broadband [formerly Road Runner or MediaOne] does NOT support Eudora -- only MS products. What they may not know is that ATTBI's instructions for re-configuring Eudora to work with ATTBI contain a very peculiar instruction in lines 10 and 17 = suggesting that you MUST select SECURE SOCKETS WHEN RECEIVING.

This is in fact NOT TRUE, as David Reed helped me to discover last night.

If you do follow their instructions and select the SSL feature, you will discover that your RETURN address MUST be the same as your LOGIN name.

This, obviously prevents a return address other than the ATTBI domain. So, if you have your own domain and wish to use it in the RETURN

field in

Eudora, do NOT select the SSL functions in steps 10 & 17 of ATTBI's online instructions -- see their web site.

Trying to be a good dooby, I explicitly followed ATTBI's online instructions, only to discover the above problem. When ever I tried tied to use <,jock@jockgill.com> as my return address, I got error 553 from the ATTBI servers.

Calls with very long wait times to ATTBI, and chats with them online, were fruitless to the point of their suggesting the 553 error message was an Eudora problem. The ATTBI techs had no idea what so ever about the relationship between the so called SSL requirement and its effect to force you to use your ATTBI login in name for your return address.

Makes you wonder why we ever trust large organizations. As David might say, the power of the edges to collectively organize around problems solved this problem in very short order -- once I gave up on the old notion of turning to the central authority.

Jock Gill < jock@jockgill.com > <www.jockgill.com <<http://www.jockgill.com/>> >

Interactive Digital Studies

[For Dave's IP archives see:

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

]

## **⚡ 'Phantom Menace' typing is just a Microsoft speech feature**

Hawkins Dale <rhdale@yahoo.com>

*Tue, 12 Mar 2002 13:30:48 -0800 (PST)*

Slashdot (slashdot.org) and others are reporting that "some Windows XP users are finding random words inserted into their text as they write. The problem is caused by XP's speech recognition system, which is turned on by default by some manufacturers. It's listening to the random noise you get even when the mic is turned off."

Microsoft is blaming the problem on some computer manufacturers who enable this feature by default in their installation of the operating system.

Draw your own conclusions regarding the risks of adding powerful features that users are unaware of.

Hawkins Dale

---

## **⚡ Re: Yet another case of a program changing your input ([RISKS-21.94](#))**

Gene Wirchenko <genew@mail.ocis.net>

*Tue, 12 Mar 2002 08:16:44 GMT*

Funny. On Sunday, I was doing an Excel tutorial as part of an accounting course. The tutorial was setting up a grades spreadsheet system. I ran into the same problem of short grades being overridden by longer

ones!

Then there was Word miscorrecting a word in an e-mail address for me recently. Unfortunately, the lab computers at my college have the Word settings set so that spelling corrections are automatically accepted. While this can be turned off, it must be done every login. What a bother.

My college is University College of the Cariboo. The domain is cariboo.bc.ca. Word miscorrected "cariboo" to "caribou". I'm glad that I noted it as it happened as this was on my resume for co-op.

Just to add to the fun, Word does some substitutions. Try typing a line with a number of asterisks. Word will replace it with blocks. Sometimes, you can delete this line. Sometimes, you can't. I have also had horizontal lines inserted that I couldn't get rid of. I had a draft for a report that I had to retype, because I couldn't get rid of the lines.

Gene Wirchenko

---

## **✶ Re: Air Force seeks better security from Microsoft**

tom poe <tompoe@renonevada.net>  
*Tue, 12 Mar 2002 10:14:54 -0800*

> "The military and the government don't really have too much choice at  
> this point except to start to put pressure on Microsoft and others to  
> improve software security," Erbschloe says.

Hi: Well, Erbschloe, you're wrong. You have an easy, easy choice to make.

If \$13 Billion in taxpayer losses isn't enough to switch OS and tighten

security for the Air Force, there's something terribly wrong in the Computer

Economics workshop?!! Thanks, Tom

---

**✶ Re: Air Force seeks better security from Microsoft (Poe, [RISKS-21.95](#))**

Jei <jei@cc.hut.fi>

*Tue, 12 Mar 2002 19:25:58 +0200 (EET)*

Sounds to me like we need a law that empowers the consumers to demand their money back if the products prove to be faulty.

But didn't the US lawmakers just make a law that empowers the software makers to enforce whatever licences they like?

Software quality will not only get worse, but it will be impossible to publicly state that it sucks. Publishing security holes will also likely be equal to legal suicide.

The only thing we'll get is a public mirage of better security and functionality, while in reality things will actually be a lot worse.

Oh well.

## Disclaimers

"Michael (Streaky) Bacon" <streaky@baconsonline.com>

*Tue, 12 Mar 2002 07:47:47 -0000*

A friend sent me the following disclaimer at the end of an e-mail he received from a contact in the BBC (British Broadcasting Corporation). It reads (in part):

"Please note that the BBC monitors e-mails sent or received. Further communication will signify your consent to this."

Now this presents a dilemma because, merely by responding, you consent to the monitoring - making it challenging to refuse whilst keeping a convenient and effective communication channel open.

Anyway, if the external correspondent uses (say) telefax and the internal correspondent uses e-mail -- is that "communication".

If one does not consent (and can successfully communicate this without compromising one's position), can one's internal correspondent continue to send me e-mails - without them being monitored?

Further, since the first part of the 'disclaimer' says that, "the BBC monitors e-mails sent", there is the unanswered question, "Was the original e-mail monitored - WITHOUT the recipient's consent?"

Additionally, what constitutes a 'response'? If the original message had requested a 'read' or even 'received' response - often automatically sent --

would this be a 'consent' to the monitoring?

Differences between 'opt-in' and 'opt-out' are exploited by marketers (see several other threads, most recently Knox, [RISKS 21.94](#)), but RISKS arise when those who write disclaimers are ignorant of the technology involved.

Also, why pick on only one form of communication? How long before the 'thought police' in the BBC extend their monitoring to the telephone, telefaxes and letters?

Michael (Streaky) Bacon

---

## **✶ Re: Loosing It's Grammer Skill's (Searle, [RISKS 21.94](#))**

"Michael (Streaky) Bacon" <streaky@baconsonline.com>  
*Tue, 12 Mar 2002 07:18:22 -0000*

I recently reviewed some pages on the Web site of a major computer manufacturer and, among other issues, found several solecisms, grammatical errors, strange and tortuous phraseology, mixed persons, typographical errors and differences in how separate hypertext links to the same 'off site' page were treated. A particular classic was: "... challenges of reliability, scalability, and manageability that are needed ..." -- I hadn't realised that anyone \*needed\* challenges!

On enquiry I was told that no-one reviewed for content, as the pages were

written by subject matter experts. Any reviews were to check conformance with corporate presentation style. But even that alleged check missed the incorrect presentation of the company name in one instance.

SMEs may know their subject, but clearly that isn't grammar, law or risk management.

The risks are manifold, and include: inappropriate material being accidentally or deliberately posted; the company being committed to do something they never intended to do; corporate liability being attracted in a manner that is not properly (risk) managed; any corporate commitment to quality being thereby degraded.

Michael (Streaky) Bacon

---

## **Re: Loosing It's Grammer Skill's (Searle, [RISKS 21.94](#))**

Klaus Brunnstein <brunnstein@informatik.uni-hamburg.de>

*Tue, 12 Mar 2002 09:54:21 +0100*

Concerning Greg's complaint about some impact of contemporary publication support software qw cause in reducing the quality of English (or AmGlish?) writing, another -- possibly more serious -- cause may be related to what I call the "imperialism of English": when multi-million non-native English speakers and writers are forced to use English as communication vehicle, how can someone assume that "quality English" may result? Moreover, differences

between "island English" and "American English" may also contribute to bad grammar (as well as manuals even from English companies).

On the other side, we observe that German students use publication software to produce better looking papers though at significantly lesser grammatical quality. This tendency which is also observable in schools may not only be attributed to usage of IT!

My 2 cents (yes, we have also cents in Germany now), with my apologies for possibly bad grammar and expression :-)

Klaus Brunnstein (March 12, 2002)

---

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

<albaugh@spies.com>

*Tue, 12 Mar 2002 08:25:13 -0800 (PST)*

> ... "Driver's Wanted"

I believe Greg has misunderstood. They are trying to warn you that they are a "family business", and that there are outstanding warrants for the driver of this cab. Perhaps you will choose this cab for a sense of adventure.

Perhaps you will decide that arriving at the airport with a half-dozen police cars in hot pursuit is not your cup of tea. Either way, you have to applaud their honesty.

## ✉ **Re: Loosing It's Grammer Skill's (Searle, [RISKS-21.94](#))**

"Merlyn Kline" <merlyn@zyweb.com>

*Tue, 12 Mar 2002 10:25:35 -0000*

[I omitted a comment on "Driver's Wanted" similar to Mike Albaugh's preceding message. PGN]

[...] as you point out:

> Sure, I know what they really mean,  
> and

> English is defined by its common usage over an extended period  
> of time.

So what's the problem? Sure[1], it's annoying when the language drifts away from the dialect you had hammered in to you at school, but that's life. It's not wrong; just different. If you want annoying, you should try being a British English speaker reading Risks![2] In fact, as has been mentioned on Risks before, there are actual risks here: e.g. American English has lost the distinction between "ensure" and "insure". Here in Britain, I'm happy to deal with someone who ensures risks won't be realised, but not so happy to deal with someone who just insures. In America, I can't tell which is which. One of my favourite examples of this type of error is a notice in a local music store that says "CDs cannot be returned for a refund. This does not effect your statutory rights." (No, I bet it doesn't!). I'm not sure this is even an error in America, let alone funny[3].

The evolution of language is driven by a fantastically complex and ultimately self-correcting system. If (e.g.) the taxi firm starts to suffer because everyone thinks their drivers are wanted criminals, eventually there will be another drift in the language to enhance the distinctions between possession, plurals and elision.

Anyway, isn't your complaint really about the failings of an education system that is apparently incapable of helping its clients understand the simple rules related to the use of apostrophes in English?

> Are we doomed to accept bad grammar as the official standard?

We are :(  
Chaucer, even Shakespeare, would be horrified by what we call English.

Merlyn Kline

[1] Arrgh! I'm drifting into American English idiom! The power of context!

[2] Perhaps you are. See [1].

[3] OTOH perhaps I am misled by the ever increasing abuse of these two words, and the distinction remains in American English as well as British. I'm not sure.

---

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

Dave Williams <dave\_williams@compuserve.com>  
Tue, 12 Mar 2002 14:31:28 +0000

You are talking about the rise of the Apostrophe Virus (also known in the UK as the Greengrocers' Virus, because the misplaced apostrophe only used to appear on hand lettered signs in fruit and vegetable shops)

The rise of DIY publishing, in print and on the Web, has propagated this virus to the point that it now appears in national newspapers, advertisements, and on major Web sites; all published by people who ought to know better. The problem is compounded by the long-term shift to a less literate culture, where words are less cared for, and spellcheckers are assumed to handle all grammar issues.

As people see the misplaced apostrophe more and more in established media, the virus becomes legitimised, and so they are more likely to use an apostrophe, on the principle that it's best to put it in just in case

The probable future is that in time, the use of the apostrophe-s will become the default for all occurrences of the letter s at the end of a word. So we are soon likely to assume it's normal to see apostrophe's at the end of word's, even though reader's of mature year's might think it suck's.

Dave Williams (or should that be William's?)

[DIY = Do-it-yourself, a.k.a. samizdat, which might inspire a self-publishing outfit called Sammy's.Dot.com? PGN]

---

**✉ Re: The RISK of ignoring permission letters (Knox, [RISKS-21.94](#))**

Rob Slade <rslade@sprint.ca>

Tue, 12 Mar 2002 11:18:53 -0800

Our recommendation in regard to spam, for those who did not want to expend the time and effort required to track down the spammer and his upstream provider, has always been to ignore it. This new style of spam is rather more problematic. The United States now has a slew of legislation in regard to spam: various states have their own, and I believe that there is federal legislation as well. The legal questions boggle the mind. Is this just another address harvesting scheme, like the old "reply to this message if you want off the list" types? Does a failure to respond to this message constitute a legitimate "acceptance" on my part? (Particularly for those of us from outside the US?)

> This is NOT requesting permission. This is warning you that by NOT  
> responding, you are implicitly consenting to them sending you spam. With  
> UCITA, this might even become legally acceptable (like click-wrap licenses).

Yet another twist to the legal questions. Would this kind of thing be legal in Virginia?

> Finally, note how they try to play it cool in the last paragraph, talking  
> about how I 'requested' to be notified of special offers.

Apparently I've done all kinds of things on the net that I've never actually done. I've even been signed up in some weird kind of pyramid/

mlm scam that  
I've never heard of ...

rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca  
pl@canada.com  
[http://victoria.tc.ca/techrev](http://victoria.tc.ca/techrev/~rslade) or [http://sun.soci.niu.edu/](http://sun.soci.niu.edu/~rslade)

---

**✶ Re: The RISK of ignoring permission letters (Knox, [RISKS-21.94](#))**

"Greg Searle" <greg\_searle@hotmail.com>  
*Tue, 12 Mar 2002 08:34:58 -0500*

The best thing that you can do when you receive this type of message is to REPORT IT. This message itself is unsolicited e-mail. If you report it to the ISP that it was sent through, then the ISP may enforce its Acceptable Use Policy, and make the offending company think twice about this practice. Spammers are good liars. Call the lie and report the abuse, pointing out that you DID NOT request the message.

---

**✶ Re: The RISK of ignoring permission letters (Knox, [RISKS-21.94](#))**

"George C. Kaplan" <gckaplan@ack.berkeley.edu>  
*Mon, 11 Mar 2002 16:38:34 -0800*

> With UCITA, this might even become legally acceptable ...  
I don't know about whether UCITA makes this legal, but it's

commonly  
accepted that such "opt-out" links don't actually remove you  
from the  
spammer's mailing list. Instead, they confirm that there's a  
real person  
reading e-mail sent to your address, thus ensuring that you'll  
end up on  
\*more\* mailing lists.

> Finally, note how they try to play it cool in the last  
paragraph, talking  
> about how I 'requested' to be notified of special offers. This  
is an  
> outright lie.

If they lie to you about this, don't you think they'll lie to  
you about  
what their opt-out link does?

George C. Kaplan, Communication & Network Services, University  
of California  
at Berkeley 1-510-643-0496 gckaplan@ack.berkeley.edu

---

## **✶ Re: The RISK of ignoring permission letters (Knox, [RISKS 21.94](#))**

"Michael (Streaky) Bacon" <streaky@baconsonline.com>  
*Tue, 12 Mar 2002 07:27:05 -0000*

This presents a compound RISK. On the one hand, not replying  
appears to  
give consent to continuing to receive e-mail; on the other hand,  
replying  
confirms your e-mail address - which can then be resold as a  
legitimate,  
active, human-attended address.

Michael (Streaky) Bacon

## ✦ **Re: Welland Canal Bridge runs into ship ([RISKS-21.61](#))**

Dave Gillett <dgillett@deepforest.org>

*Tue, 12 Mar 2002 14:08:06 -0800*

The freighter Windoc, which was hit by a lift bridge last summer, losing its wheelhouse and funnel and catching fire, has made the news again.

Windoc was apparently one of twelve freighters wintering over in Hamilton harbor, and one of three of those to break loose from their moorings in 130 kph winds last week. The ship drifted for about 5 km before grounding close to a major highway.

No obvious computer connection, just follow-up on an old item....

---

## ✦ **Re: LED lights can reveal computer data (NewsScan, [RISKS-21.94](#))**

Nick Simicich <njs@scifi.squawk.com>

*Mon, 11 Mar 2002 22:07:41 -0500*

It is not quite true that no one has looked at reading computer data from LEDs before. In the 1990 timeframe, there was a brand of scuba computer called the Orca Delphi that would dump recordings of your depth profiles to a LED which normally functioned as a decompression warning LED. You put it in dump mode by disconnecting the power (9v lithium or alkaline

battery) and reconnecting it within a few seconds.

As you can imagine, most diving computers are designed on the "KISS" principle. Errors in these computers could cause a life threatening condition - by incorrectly calculating your decompression obligation, they could put you at risk. An inexperienced diver might not detect that the answers that the computer was calculating was wrong. But they are purposely simply devices. They may not even have an "on" button, for example---they may turn on in response to water pressure, conductivity, or, in the case of this computer, the fact that you turned on your air (this computer also tried to estimate how much air you had left in minutes based on how rapidly you were using it, so it had a high pressure air connection). This frees you from the task loading of having to remember to turn the computer on. Many do not have an off switch - once they determine that you have "completely decompressed" according to their mathematical model, they turn off automatically. The point here was that the engineers did not want to add the complexity of an extra electrical interface to this computer for dumping - they wanted two inputs, the water pressure and tank pressure transducers, one power input, and the lcd panel for output. And the LED to call your attention to warning issues. The point was to try and get a second use out of this LED as a data output device.

In any case, the company had promised a dump device for the computer and

never delivered. The method of memory dumping was not initially announced, although they eventually mentioned, at a lecture, that it was going to be a "light pen". Someone noted that under some circumstances, disconnecting and reconnecting the power to the computer (it was a nine volt battery) caused the LED to light up for a few seconds at half brightness. I made a call to the engineer and he admitted that yes, that was their planned dump method -- they flashed the LED at 2400-8-N-1, and simply dumped the memory. The dump was in this format:

```
>000 C7 FF C0 48 C0 01 8D A5 8D A0 C7 FF C0 47 C0 07
>010 89 97 8D 9A 84 40 84 33 80 2E 80 2B 80 2C 80 2D
```

...and so on. That is, it dumped in ascii characters, complete with offsets at the beginning of each line, and a crlf at the end.

There was a checksum for some of the memory, but not much of it.

I'm not an electronics person, and, whereas there were circuits published (on rec.scuba), we were never able to get anything that worked reliably. We tried the approach of reading the LED directly, and it was difficult to hold the detector in the exact alignment required for the duration of the dump. It was actually so difficult to get a good dump by reading the light from the LED that we built a circuit that measured battery voltage instead. The company engineers had the same problem, I heard. I also heard that they had problems getting consistent readings because of LED brightness differences and positioning under the faceplate. The engineer suggested the battery

method to me - and whereas I was able to breadboard a circuit and get a dump with it, I was not enough of an electronics person to be able to build one that would adapt to various battery voltages - mine would only work with a fresh lithium battery and an oscilloscope for tuning.

Obviously, Loughry has a great deal more skill than we did in reading these LEDs.

Search google in rec.scuba for the words "orca delphi dive dump device".

There are some posts from 1990.

Nick Simicich - njs@scifi.squawk.com

---

**⚡ Re: LED lights can reveal computer data (NewsScan, [RISKS-21.94](#))**

<peter@whirled-routers.com>  
*Mon, 11 Mar 2002 15:53:49 -0800*

I'll believe it when I see it.  
The articles actually state, that no one got it to work yet.  
Until then : FUD !

Peter B.

Whirled Routers, 200 Pier Ave. Suite 39, Hermosa Beach, CA 90254  
USA  
310 376 8755 / fax 8785

---

**⚡ REVIEW: "Incident Response", Kevin Mandia/Chris Procise**

Rob Slade <rslade@sprint.ca>

Tue, 12 Mar 2002 07:49:30 -0800

BKINCDRS.RVW 20020108

"Incident Response", Kevin Mandia/Chris Procise, 2001, 0-07-213182-9,

U39.99

%A Kevin Mandia mandiak@erols.com

%A Chris Procise authors@incidentresponsebook.com

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

%D 2001

%G 0-07-213182-9

%I McGraw-Hill Ryerson/Osborne

%O U\$39.99 905-430-5000 fax: 905-430-5020

%P 509 p.

%T "Incident Response: Investigating Computer Crime"

Part one is supposed to provide us with the basics of incident response. Despite the assertion, in the introduction, that such response deals with much more than computer crime and that incidents can vary widely, chapter one details a deliberate and malicious intrusion into a computer system, by an incredibly inept attacker, using inside information. Chapter two provides a definition of incident response, but it does lean heavily towards crimes, law enforcement involvement, and directed attacks. The material also assumes that an incident response team can be called upon or formed at short notice. The suggestions for advance preparation, in chapter three, do cover a broad range, but the writing is not always organized, and the material has gaps and covers many topics superficially.

Part two purports to deal with technical issues. Chapter four deals with guidelines for investigations, but, again, concentrates only on directed attacks from outside the organization. The computer

forensic

process, in chapter five, is limited to retention and copying of evidence. There is a rather terse review of Internet Protocol header

information in chapter six. Chapter seven lists some information related to network monitoring and logging. "Advanced Network Surveillance" (chapter eight) examines a few of the more convoluted exploits.

Part three describes operating system functions associated with system investigation. Chapters nine to twelve list a number of utility programs that can be used to obtain system information.

Part four is a grab bag of material dealing with special topics, chapter thirteen dealing with routers, fourteen the Web, and fifteen various servers. A number of security and security breaking tools are enumerated in chapter sixteen.

The emphasis in this book is adversarial: seeing incident response as primarily a matter of active defence against an active attacker. Most companies will probably see incident response as a matter related to technical support: an endless stream of incidents, most of which are trivial, and a select few of which indicate serious problems. As such, the book does, occasionally, point out some matters to consider, and possibly new practices to adopt in order to deal with those isolated events that are important enough to turn over to law enforcement agencies. However, overall, the text does not provide much guidance in preparing for and responding to serious incidents.

copyright Robert M. Slade, 2002 BKINCDRS.RVW 20020108  
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/>



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 21: Issue 96**

**Thursday 14 March 2002**

## Contents

- [Airbus A300 "BSD" Incident from 1997](#)  
[Peter B. Ladkin](#)
- [Airbus A320 Cross-Wired Sidestick Incident](#)  
[Peter B. Ladkin](#)
- [Out with pilots, in with pibots](#)  
[Erling Kristiansen](#)
- [Risks of Unicode and WSIWYG](#)  
[Len Spyker](#)
- [Thousands seek Ladonian citizenship over the Internet](#)  
[PGN](#)
- [Risks of inadequate testing, yet again](#)  
[Tony Lima](#)
- [Hacking with a Pringles tube](#)  
[Chris Leeson](#)
- [Re: LED lights can reveal computer data](#)  
[Tramm Hudson](#)  
[Colin McEwen](#)
- [Re: Loosing It's Grammer Skill's](#)  
[Mike Albaugh](#)
- [Re: Sorry, that number is now in service](#)

[Jay D. Dyson](#)

[Gene Spafford](#)

[Jay D. Dyson](#)

[James Graves](#)

[Gene Spafford](#)

● [Re: Disclaimers](#)

[J F Hitches](#)

● [Info on RISKS \(comp.risks\)](#)

---

## ✂ Airbus A300 "BSD" Incident from 1997

"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>

*Thu, 14 Mar 2002 16:36:11 +0100*

During the course of trying to figure out why AA587's tail came off, the US NTSB is looking at an incident to another Airbus A300-600 aircraft in 1997, also in service with American Airlines. AA Flight 903, en route from Boston to Miami on 12 May 1997, experienced an upset after descending to 16,000ft in preparation for landing. The NTSB determined that the aircraft stalled, and entered pitch, yaw and roll manoeuvres described as "oscillations" which continued for 34 seconds before recovery. The aircraft lost 3,000ft altitude during the event. The NTSB also determined that the crew took "improper remedial action" after the aircraft was allowed to stall. One person was seriously injured.

Aviation Week (4 Mar 2002, pp52-3) says that investigators learned that flight data displayed on the Electronic Flight Information System (EFIS)

screens disappeared for 2-3 sec. during the upset while the avionics reset. "Data were replaced by white diagonal slash marks across the screens." That means that the crew lost essential flight data: attitude, airspeed, rate of descent, altitude, etc. This data would normally be essential to proper recovery from an "unusual attitude", particularly at night and in clouds. (The AvWeek article does not state the time or weather conditions.)

As a consequence, the NTSB issued safety recommendations A-98-3, through -5. A-98-3 asked the FAA to require modification of the Symbol Generator Unit software so that "unreliable data reset of the [EFIS] will not occur during an upset". The SGU renders the flight data on the EFIS screens from sensor and other input. The NTSB says it "learned that the threshold for triggering an auto reset can be reached during an inflight upset. For example, if the roll angle rate of change is more than 40 deg. per sec., a reset will occur." According to the Flight Data Recorder, this limit was reached during the upset.

Peter B. Ladkin, University of Bielefeld, Germany  
<http://www.rvs.uni-bielefeld.de>

---

## **✈ Airbus A320 Cross-Wired Sidestick Incident**

"Peter B. Ladkin" <ladkin@rvs.uni-bielefeld.de>  
*Thu, 14 Mar 2002 19:32:36 +0100*

On 20 Mar 2001, a Lufthansa Airbus A320 destined for Paris came within two feet and a few seconds of crashing on takeoff from Frankfurt.

The captain (in the left seat) was Pilot Flying (PF) on takeoff. Shortly after leaving the ground, the aircraft encountered a little turbulence and the left wing moved down. PF corrected, applying "right stick", but the aircraft responded by rolling further left. Left bank reached 21 deg. and the left wingtip came within 1.5 feet of the ground. The first officer, Pilot Not Flying (PNF), realised what the problem was, switched sole control to his stick (normally, the control inputs from both sticks are averaged) and recovered the aircraft. The crew climbed the aircraft to 12,000ft, performed some handling checks to confirm that the captain's stick was operating in the reverse sense in roll, and landed back at Frankfurt.

Control reversals of this sort are known with conventional aircraft, in particular, small aircraft with cables between cockpit controls and aerodynamic control surfaces. Cables are reconnected in reverse during maintenance. It pays to check the controls thoroughly and carefully after maintenance (in fact, one is required to check them before every flight). Not everyone can recover - has recovered - either themselves or the aircraft from the surprise of suddenly having to deal with controls operating in reverse sense upon takeoff.

But the A320 is fly-by-wire, not fly-by-cable. It turns out that the

captain's controller had indeed been reverse-connected (electrically) for roll commands, during maintenance. And the first officer's was correct. With cable control, if one is wrong, then both are wrong. In either case, this should be noticed on the control check before takeoff.

The incident raises three main questions:

1. How did the misconnection happen?
2. Why did maintenance not discover it on the return-to-service control check (after controls have been worked on, such a check is mandatory)?
3. Why did the pilots not discover it on the pre-takeoff control check?

Sidestick roll commands are input into five computers: two Elevator and Aileron Computers (ELACs) and three Spoiler and Elevator Computers (SECs).

Each of these boxes is "dual channel", with two processors, one hot and the other shadowing the first. Each ELAC contains a pair of MC68000 series processors with dissimilar software; each SEC a pair of Intel 80186's with dissimilar software. For roll, the ELACS control the ailerons, and the SECs the spoilers, on the wings, through three different hydraulic systems. Roll is achieved through use of the four outer spoilers (of five, per side) and ailerons (two adjacent, outboard of the spoilers, per side), and actuation of these surfaces is distributed amongst the hydraulic systems to achieve redundancy amongst the hydraulics. Control command redundancy is achieved by distributing the control surfaces amongst the computers, through different hydraulic systems. One can even lose both ELACs and roll is then controlled

by the SECs, and vice versa. A diagram and explanation can be found on pp. 133-4 of Cary R. Spitzer, *Digital Avionics Systems: Principles and Practice*, Second edition, McGraw-Hill, 1993.

The incident aircraft had returned from maintenance. According to the report by David Evans in *Air Safety Week (ASW)*, 4 Jun 2001, maintenance personnel had found a damaged pin on one segment of the four connector segments on the "rack side" of one of the ELACs. Each connector segment has 140 pins. ASW says that a complete rewiring "upstream" of the connector pins was performed. Apparently the polarity was reversed on four wires in one segment: two for roll control inputs and two for the associated control channel outputs. Although it is physically impossible to mismatch connectors, it is mooted that there are some differences in color-coding of the wiring between different aircraft models and that this may have played a role.

But this story conflicts *prima facie* with the details of the architecture and the incident history. The sidestick input goes into five computers, which amongst other things vote somehow on consistency. If only one ELAC received reversed control commands through reversed wiring, it would have conflicted with the other and they would have been taken off-line, leaving the SECs with (correct) control. Generalising, it follows that a majority of the five ELAC and SEC computers were operating with reversed control from the left sidestick during the incident. The reversed connection must have

been effected upstream of the point or points at which the one control signal from the sidestick is demultiplexed into the five signals for the five computers. If a connector and the associated wiring to one ELAC was faulty, I do not see why that should require a rewiring upstream of any demultiplexor. I do not see how such a rewiring can have affected signals to all five (or even a majority of all five) computers.

(The other possibility is that the signal from the sidestick is not demultiplexed; that each computer receives a separate signal direct from the sidestick. But that would require at least ten pins on the sidestick connector - two for each computer - and only four wires were reported misconnected; even those were in a two-plus-two arrangement. So that could not have affected the senses of the other six.)

It has been confirmed that, after maintenance, the technician performed control checks only on the right-seat sidestick, not the left-seat stick. It makes no sense to me why, after performing maintenance on the left-seat sidestick, anybody (let alone a Lufthansa technician) would then perform checks only on the \*right-seat stick\*. If you have just repaired a flat tire on your car, you don't inflate the tire on the other side! That suggests some cognitive confusion, namely that the rewiring did not take place right up to the sidestick, but up to an intermediate connector that was imagined to be common to both sticks. But, as I have just noted, I just cannot reconcile that supposition with the avionics architecture and

the rest of  
the story.

The preflight checks require both pilots to perform a control check. When the check is performed, a schematic of the control surfaces (the "Flight Control Page") appears on the screen of the Electronic Centralized Aircraft Monitor (ECAM), and the actual control outputs are shown. The ailerons and spoiler actions would have been shown reversed. Upon performing a control check in this situation, it is just conceivable that one might not notice that the ailerons are operating in reverse sense, but the spoilers are asymmetric: one side goes up and the other doesn't move. I cannot imagine putting in left stick and then just not noticing that the \*right spoiler bank\* activated instead of the left bank, or vice versa. So there is another puzzle. And if some of the computers were computing differently-sensed control commands from others, one would have expected that an annunciation on the ECAM to that effect would have followed, and that the annunciation would have been noticed by both pilots.

In the ensuing ten months, I have obtained no information which sheds further light on this incident.

There are two kinds of issues here. One kind admits possible explanations: maybe the humans failed in a big way on their post-maintenance and pre-flight checks somehow. The other kind does not admit any explanation: I see no way to reconcile the supposed details of the misconnection in this

incident with the architecture and operation of the ELAC and SEC avionics.

The story must be different from that which has been told, but I do not know how.

Peter B. Ladkin University of Bielefeld, Germany

<http://www.rvs.uni-bielefeld.de>

---

## **✶ Out with pilots, in with pibots**

<Erling.Kristiansen@esa.int>

*Thu, 14 Mar 2002 09:43:18 +0100*

>From AVflash 8.11b. <<http://www.avweb.com>>

Later this week, representatives from NASA, the U.S. Navy, New Mexico State University and the industry will descend upon Las Cruces, N.M., to show that remotely controlled aircraft can operate safely in the National Airspace System. The team will fly up to three aircraft on collision courses to test onboard sensor technology designed to detect and avoid potential threats. The Proteus aircraft, built by Scaled Composites in Mojave, Calif., will take part, fitted with a Skywatch HP traffic advisory system, a radio-based device that detects other aircraft. Proteus will also carry an Engineering 2000 infrared sensor, and an Amphitech radar "non-cooperative" sensor -- devices that don't require signals or transmissions from any other source -- to detect the presence and course of other aircraft.

[Gives me a nightmarish vision of a cloud of little unmanned aircraft all heading for the same place, trying to avoid each other, and the regular, piloted airliner flying through the cloud and scattering it in all directions - pretty scary. EK]

---

## ✶ Risks of Unicode and WSIWYG

Len Spyker <redmond@inet.net.au>  
*Wed, 06 Mar 2002 21:00:35 +0800*

My daughter was finally called in to aid with a help desk call from a Japanese visitor to Perth Australia. He was setting up his Mac to connect to a local ISP with a package the ISP had supplied.

The visitor was entering into the dialog boxes the usual english texts "mail@fred.com etc" but it would not connect. Many phone calls to the support desk were futile.

Then my clever bilingual daughter who uses a Japanese OS Mac herself finally realised the Mac user was probably in some Japanese text mode? when entering the "English" looking characters into the boxes. When she got him to change to a pure English text mode and entered it all again it worked!

I guess that when the connect strings went out instead of sending 4 ASCII bytes for "fred" it was sending out 4 unicode 16 bit codes, or 8 bytes.

The OS was storing the visibly "English" text somewhere as unicode and the modem string handler was just sending out a (8 byte) null terminated string.

Maybe the problem was that the ISP's application was not Unicode aware, but definitely a really nice case of WYSINWYG. What You See Is NOT What You Get.

---

## ✶ Thousands seek Ladonian citizenship over the Internet

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

*Wed, 13 Mar 2002 12:10:12 PST*

Lars Vilks, state secretary of Ladonia, reports that more than 3,000 Pakistanis recently applied for Ladonian citizenship over the Internet. According to an 11 Mar 2002 CNN.com SCI-TECH report, Ladonia already has 6,000 registered "citizens". According to the official national Web site (<http://www.aim.se/ladonia>), Ladonia is one square kilometer in size, between Sweden and Denmark, having become a free nation on 2 Jun 1996. Its capitol is Wotan City, with one main wood building (Nimis) and a nearby town (Arx) with a stone and concrete construction. The national anthem is performed by throwing a stone into water. Having been swamped with applicants, its Web site was temporarily shut down -- because applicants had mistakenly expected jobs and housing. The on-line citizenship application has now been amended, with an appropriate disclaimer. Common

citizenship is  
free; nobility costs \$12, and you can choose your own title.

In actuality, Ladonia exists only on the Internet and in Vilks' imagination.

According to the CNN report, Vilks established Ladonia on 2 Jun 1996,

protesting Swedish authorities who had attempted to remove his two large abstract art works (Nimis and Arx?) from Skaane in southern Sweden.

Please get your April Fool's Day items in early. This is not one of them.

Everything above is true, except possibly my question-marked supposition about the identity of the disputed art works.

---

## ✶ Risks of inadequate testing, yet again

Tony Lima <TonyLima2@att.net>

Wed, 06 Mar 2002 18:46:11 -0800

I received the message shown below from Worldnet. Note the quoted first

line. I absolutely refuse to use any mail reader that "supports" html.

However, everything after <META- in the message below appears as an html box

in Agent. In other words, unless your mail reader supports html you will

never see the message telling you what to do! Perhaps AT&T should have

tested this on someone who actually uses software that doesn't support

html. - Tony Lima

On Wed, 6 Mar 2002 20:11:03 -0500 (EST), attwns-announcement-system

<CustomerNotifications@worldnet.att.net> wrote:

>To: AT&T WorldNet Customers <WorldNetCustomers@att.net>  
>Subject: Your March Newsletter Is Here!  
>From: attwns-announcement-system  
<CustomerNotifications@worldnet.att.net>  
>Date: Wed, 6 Mar 2002 20:11:03 -0500 (EST)  
>  
><META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=iso-8859-1"><!-- If your e-mail tool doesn't support html, please see the on-line version at <http://www.att.net/perks/newsletter/> -->

---

## **Hacking with a Pringles tube**

"LEESON, Chris" <CHRIS.LEESON@london.sema.slb.com>

*Fri, 8 Mar 2002 14:43:38 -0000*

>From the BBC News Website:

[http://news.bbc.co.uk/hi/english/sci/tech/newsid\\_1860000/1860241.stm](http://news.bbc.co.uk/hi/english/sci/tech/newsid_1860000/1860241.stm)

The article notes that an antenna for eavesdropping on Wireless Networks can be created out of an old Pringles tube.

A link from this article goes to a page describing how such an antenna can be made (this article by Rob Flickenger). It is written

in a partly humorous vein, and is well worth a glance:

<http://www.oreillynet.com/cs/weblog/view/wlg/448>

This is of interest to RISKS not so much for the security/privacy risks inherent in a wireless network (see RISKS Passim), but for how easy and cheap it is to create the tools for the job.

The ability to create antenna "out of anything" is nothing new:  
I remember  
my Antenna Theory lecturer describing how a satellite dish could  
be created  
out of an old metal dustbin lid. That was about 20 years ago.

---

## ✶ Re: LED lights can reveal computer data (njs, [RISKS-21.95](#))

Tramm Hudson <hudson@swcp.com>

*Wed, 13 Mar 2002 04:39:52 +0000 (UTC)*

A few years ago, my group at Sandia National Labs was building a new operating system for the Intel Paragon massively parallel super computers.

These machines had an amazing high-speed message passing interconnect, but it was flakey while we were rebuilding the network driver.

The nodes were nearly "embedded", with only the mesh interconnect and a few LEDs on the front panel. They had no other IO, not even a serial port.

There was an even more unreliable channel used for downloading kernels, but it failed as often as the mesh driver.

To help get crash data off the nodes, we wrote an ISR that would translate

printf() calls into 2400 N81 pulses of one of the front panel LEDs. We used

a 4k ring buffer, so it would continuously repeat until the machine was

reset. A light pen was duct taped over this LED and hooked to a nearby

SPARCstation's serial port. We used this for debugging for several years

and through many versions of the operating system.

The software eventually went into "production" use on the larger machine.

We occasionally saw nodes that had crashed on the big system blinking out their panic messages. Since it was installed in a secure computing facility, I was always concerned that this might be used as a covert channel for extracting data (slowly!) from the classified compute runs.

> ... and it was difficult to hold the detector in the exact alignment

We had no such problems. I seem to recall that this was working within a weekend of realising that we could do it. Most of the time was tracking down the light pen...

Recently a similar subject was discussed on alt.folklore.computers.

<a26pkf\$lji\$l@newsreader.g1.core.theplanet.net> started the thread on "Morse code diagnostics".

Trammell.Hudson@celera.com <http://www.swcp.com/~hudson/> W 1-240-453-3317

---

## ✉ **Re: LED lights can reveal computer data ([RISKS-21.95](#))**

Colin McEwen <Colin.McEwen@INTERROUTE.COM>  
*Thu, 14 Mar 2002 14:04:20 -0000*

LEDs intended as activity lights for human observation are engineered to give bright and easily perceived output when signals are detected. This requires flashing at a few Hertz max, despite the signals being

anywhere

between 2400 bps and 100+ MHz (depending on the system). The solution is to use a monostable or other pulse-stretching device in the driver. This destroys any direct relationship between LED brilliance and the data.

Direct drive of the LED with the data is not normally used - short data

bursts just are not seen at all and continuous data usually gives the half brightness effect described by Nick Simicich in [Risks-21.95](#).

I am prepared to believe that LEDs indicating modem \*status signals\* such as CTS (Clear To Send) \*might\* be directly driven by the signals, and thus \*might\* be viewed at a distance - but I am not prepared to believe that the \*data\* is exposed in this way.

[Note that many important advances in knowledge have been immediately preceded by an expert saying "this cannot be done". I am therefore making my contribution to this topic by saying "this cannot be done" (!)]

---

## ✶ Re: Loosing It's Grammer Skill's (Williams, [RISKS-21.95](#))

<albaugh@spies.com>

Tue, 12 Mar 2002 17:00:37 -0800 (PST)

> You are talking about the rise of the Apostrophe Virus [...]

Ah, but folks who read these electronic documents on anything but Windows

see not apostrophes, but question-marks or little hollow rectangles, courtesy of the exceedingly ill-named "smart quotes". That is, they do unless the author has been silly enough to include the apostrophes yet wise enough to run the text in question through John Walker's "Demoronizer". This appears to me an unlikely convergence. I have even seen cases where the offending apostrophes were completely eliminated, which would be a good thing (tm, Martha Stewart), if not for the fact that the correct apostrophes were also eliminated.

> ..., and spellcheckers are assumed to handle all grammar issues.

Only Hogwarts students really need spellcheckers, IMHO :-)

(although perhaps I am mistaken, given the Sorceror's Apprentice nature of the average Spelling Checker)

---

**✉ Re: Sorry, that number is now in service (Spafford, [RISKS-21.92](#))**

"Jay D. Dyson" <jdyson@treachery.net>  
*Fri, 22 Feb 2002 16:28:45 -0800 (PST)*

I read with interest Gene Spafford's tale regarding his friend's addressing within the 69 Class A netblock. I just did a quick rifling both the ARIN database and the IANA IPv4 Addressing Space, because I too have my routers and firewalls similarly configured.

It would seem that both ARIN AND IANA are just as unaware of the assignment of the 69/8 netblock as Gene was. Both list the 69 through 79

Class A's as "Reserved."

I think this merits further investigation.

---

**⚡ Re: Sorry, that number is now in service**

Gene Spafford <spaf@cerias.purdue.edu>

*Fri, 22 Feb 2002 19:54:53 -0500*

It was a typo in my posting. It was the 67.\* block, not 69.\*

---

**⚡ Re: Sorry, that number is now in service**

"Jay D. Dyson" <jdyson@treachery.net>

*Fri, 22 Feb 2002 17:33:09 -0800 (PST)*

And the risks are apparent. ;) (Sorry, couldn't resist.)

Looks like the 68/8 was picked up a month after the 67/8, too. Time for me to update my lists...

---

**⚡ Re: Sorry, that number is now in service**

James Graves <ansible@xnet.com>

*Tue, 26 Feb 2002 20:31:06 -0600 (CST)*

[Gene Spafford writes about a problem with a router's configuration, and how he set up a periodic e-mail reminder.]

I think your RISKS example points out one of the most difficult issues with system administration: documentation.

Mr. Spafford has slapped a temporary bandage on the problem by sending himself an e-mail every 6 months, but he's just traded one risk for another.

What happens if his 'at job' (or whatever) fails? (\*) The only time he'll realize that it has failed is when he didn't need it (he remembered anyway).

And what about the ten thousand other bits of knowledge that he has in his head that helps keep his network running smoothly? Setting up at jobs for all those bits of information isn't practical.

And then, what happens when he's on vacation, and doesn't want to be disturbed? Of if he's been hit by a bus?

None of this is meant as a personal attack on Mr. Spafford. Having relied on his advice (through the printed page), I have only the highest respect for him and his efforts at computer security. It's just that his response to the situation is typical of a system administrator.

The better system administrators tend to have very good memory, which is both a blessing and a curse. It helps tremendously to not have to constantly refer back to documentation to get something done.

Unfortunately, the one-off problems (that will never occur again :- ) don't tend to get documented. The busy sysadmin feels he has

better things  
to do than spend 15 minutes writing up a problem and solution.

The real RISK with all this attitude is that as our lives become more  
complex (and dependent on technology) it will take longer and longer to  
diagnose and fix problems. And worse yet, we'll be fixing the same problems  
over and over again.

The only counter to this RISK is documentation. Every organization ought to  
have (IMHO), a central jumping-off point for documentation. There has to be  
one place for people to start looking for answers, if those answers exist at  
all.

Documentation is great, as long as it's relevant. As it gets out of date,  
it's less and less likely that people will use it. So then they'll spend  
(or waste depending on the point of view) time diagnosing and solving the  
same problems again. And in the mean time, service will suffer.

The best tool I've seen for up-to-the-minute documentation is a Wiki. If  
you can encourage the 'wiki attitude' in your organization, you'll end up  
with a really good, and relevant reference, which will go a long way towards  
improving the work.

James Graves

(\* ) Aside from software bugs, the classic reason why 'at' jobs fail is  
because people forget about them when they are moving to new machines. The  
ones that run every day are remembered very quickly if absent. But those

that only run every six months...

---

## ⚡ Re: Sorry, that number is now in service

Gene Spafford <spaf@cerias.purdue.edu>

*Tue, 26 Feb 2002 21:37:32 -0500*

Actually, I documented it in 3 places:

- \* in the configuration file, near where the rules are
- \* in a readme file in the same directory, where I keep notes for whoever maintains the file
- \* by posting to Risks so we build up community memory! :-)

Unfortunately, in first posting in [RISKS-21.92](#), I misidentified the networks involved. :-)

---

## ⚡ Re: Disclaimers

"J F Hitches" <J.Hitches@kingston.ac.uk>

*Thu, 14 Mar 2002 16:34:20 +0000*

Michael (Streaky) Bacon ([RISKS-21.95](#)) complained about the message on an e-mail from the BBC (British Broadcasting Corporation) stating that e-mail may be monitored and that further use indicated acceptance of that monitoring.

That sort of statement will be seen more widely on messages coming from the UK because it is part of a requirement of an Act of Parliament

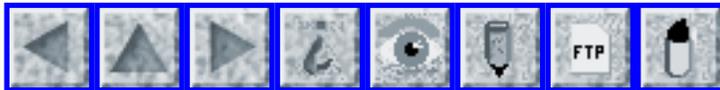
called the  
"Regulation of Investigatory Powers Act". This is combined with  
a Statutory  
instrument called "The Telecommunications (Lawful Business  
Practice  
Regulations) 2000" .

The requirement is that monitoring may only be carried out "if  
the  
controller of the telecommunications system on which they are  
effected has  
made all reasonable efforts to inform potential users that  
interceptions may  
be made".

How can one inform e-mail users other than a message on an e-  
mail?

Many of us are still pondering how we warn people who contact us  
for the  
first time.....

John Hitches



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 21: Issue 97**

**Wednesday 20 March 2002**

## Contents

- [Overcoming ICANN: Forging Better Paths for the Internet](#)  
[PFIR](#)
- [Info on RISKS \(comp.risks\)](#)

---

## ★ Overcoming ICANN: Forging Better Paths for the Internet

PFIR - People For Internet Responsibility <[pfir@pfir.org](mailto:pfir@pfir.org)>  
*Mon, 18 Mar 2002 19:21:02 -0800 (PST)*

David J. Farber  
Peter G. Neumann  
Lauren Weinstein

March 18, 2002

<http://www.pfir.org/statements/icann>

Overcoming ICANN: Forging Better Paths for the Internet

## An Open Letter to the Global Internet Community

Despite its best efforts, the Internet Corporation for Assigned Names and Numbers (ICANN) has proven overall to be a failed experiment in Internet policy development, implementation, and management. ICANN's lack of meaningful representation, and its continuing pattern of drastic and seemingly arbitrary structural and policy changes (among other shortcomings), have created an unstable and suspicion-ridden environment that is detrimental to the interests of the vast majority of Internet users around the world. The resulting overly politicized situation not only threatens the stability of the Internet itself, but also invites drastic and undesirable interventions by a variety of vested interests.

We will not in this document detail the range of specific problems and issues, which have become widely recognized and known. Key aspects of the problems relating to the Internet and ICANN have been outlined in previous statements [1][2][3], along with a set of basic proposed Internet guiding principles [4]. The continuing rapid deterioration relating to ICANN and its impact on the Internet now forces us to recommend the following three actions.

First, as an immediate temporary measure, all Internet policy, operational, and other Internet-related functions currently performed by ICANN should be transferred, as soon as practicable while maintaining continuity, to a different, already existing non-profit organization (or

organizations) on a non-permanent, strictly stewardship basis. One potential candidate we would suggest considering for this role would be the Internet Architecture Board (IAB), although there are a range of other possibilities of course. The process to plan and begin a transfer of responsibilities from ICANN should be initiated immediately.

Next, we recommend that an intensive, international study be started at once, with a mandate to propose detailed and meaningful paths for the Internet's development, operations, and management. The goal of this study would be to help guide the formation of purpose-built representative organizations and policies that would be beneficial both to established Internet stakeholders and to the wide variety of organizations and individuals who are effectively disenfranchised in the current Internet policy environment. This study should consider both short-term and long-term alternatives, and could potentially be conducted by the National Research Council (NRC) and related international organizations, among other possible frameworks.

Our third recommended step would be for the results of this study to be carefully considered and, as deemed appropriate, to be implemented. Internet-related functions would be transferred from the temporary stewardship organization(s) to the entities developed from the study results.

Time is definitely of the essence if a potential "meltdown" of

Internet

policies, functionalities, and operations in the near future is to be avoided. There is in particular an immediate need to begin the process of depoliticizing the situation and providing opportunities for consensus building regarding the range of Internet issues. Wide consensus has already been achieved on at least one key point -- even by ICANN's current president -- ICANN is seriously broken. We agree, and we additionally assert that ICANN's history, structure, and behaviors strongly indicate that the most productive course would be for ICANN's role in Internet affairs to be discontinued.

This is not to cast aspersions on the efforts of any individuals involved with ICANN in the past or present. Rather, we feel that ICANN has failed as an organization, and that the amount of "bad blood" and institutional "baggage" it carries doom "reform" efforts within the organization itself to ineffectiveness at best. We come to this conclusion reluctantly, since in the past we have considered that there might be an appropriate continuing role of some sort for ICANN. Unfortunately, this is no longer possible.

We do not have all of the answers regarding Internet issues -- nobody does.

The proposals above are not presented as any kind of fait accompli, but rather as an attempt to stimulate recognition that the Internet is facing serious problems that are in need of serious solutions. The search for solutions will be difficult, and will be a continuing effort that far transcends matters relating to ICANN. But half-measures will no

longer suffice, and the status quo (however it might be disguised or "spun") can no longer be tolerated.

Some persons genuinely fear that alternatives to ICANN might lead to situations even worse than the current dysfunctional ICANN environment. That is indeed a non-zero probability, but the increasingly chaotic situation with ICANN makes degeneration a decided \*likelihood\* if ICANN remains involved with Internet matters.

The day of reckoning is already upon us. Work should begin immediately to define and implement collaborative processes that can provide hope of assuring that the Internet will be the best possible resource for the population of the entire world. The risks in change are real, but the need for change and the possibilities for meaningful and beneficial progress are even greater. If we do not take these steps, we may well be dooming the Internet to a future of mediocrity at best, or of decay, fragmentation, greed, and even worse outrages.

[1] PFIR Statement on Internet Policies, Regulations, and Control

<http://www.pfir.org/statements/policies>

[2] PFIR Proposal for a Representative Global Internet Policy Organization

<http://www.pfir.org/statements/proposal>

[3] URIICA Announcement

<http://www.uriica.org/announcement>

[4] PFIR Declaration of Principles

<http://www.pfir.org/principles>

Sincerely,

David J. Farber

farber@cis.upenn.edu

Tel: +1 (610) 304-9127

Member of the Board of Trustees EFF - <http://www.eff.org>

Member of the Advisory Board -- EPIC - <http://www.epic.org>

Member of the Advisory Board -- CDT - <http://www.cdt.org>

Member of Board of Directors -- PFIR - <http://www.pfir.org>

Co-Founder, URIICA - Union for Representative International  
Internet

Cooperation and Analysis - <http://www.>

[uriica.org](http://www.uriica.org)

Member of the Executive Committee USACM

<http://www.cis.upenn.edu/~farber>

Peter G. Neumann

neumann@pfir.org or neumann@csl.sri.com or neumann@risks.org

Tel: +1 (650) 859-2375

Co-Founder, PFIR - People For Internet Responsibility - <http://>

[www.pfir.org](http://www.pfir.org)

Co-Founder, Fact Squad - <http://www.factsquad.org>

Co-Founder, URIICA - Union for Representative International  
Internet

Cooperation and Analysis - <http://www.>

[uriica.org](http://www.uriica.org)

Moderator, RISKS Forum - <http://risks.org>

Chairman, ACM Committee on Computers and Public Policy

<http://www.csl.sri.com/neumann>

Lauren Weinstein

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

Tel: +1 (818) 225-2800

Co-Founder, PFIR - People For Internet Responsibility - <http://>

[www.pfir.org](http://www.pfir.org)

Co-Founder, Fact Squad - <http://www.factsquad.org>

Co-Founder, URIICA - Union for Representative International  
Internet

Cooperation and Analysis - <http://www.>

[uriica.org](http://uriica.org)

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

Member, ACM Committee on Computers and Public Policy

(Affiliations shown for identification only.)



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 21: Issue 98**

**Friday 29 March 2002**

## Contents

- [Friendly Fire deaths traced to dead battery](#)  
[Jamie McCarthy](#)  
[KNHaw](#)
- [British Air Traffic Control system outage](#)  
[Alistair McDonald](#)
- [Clinton cartoon carries virus](#)  
[NewsScan](#)
- [Low-tech election risks: mice](#)  
[Mike Martin](#)
- [Black box or Pandora's box?](#)  
[Monty Solomon](#)
- [eBay identity theft](#)  
[Scott Nicol](#)
- [Software "glitch" changes the colour of the universe](#)  
[Pete Mellor](#)
- [Bioinformatics start-of-the-art](#)  
[Richard A. O'Keefe](#)
- [Windows XP disables own firewall](#)  
[Scott Miller](#)
- [Re: LED lights can reveal computer data](#)

[Anthony DeRobertis](#)

● [Re: Disclaimers](#)

[Malcolm Cohen](#)

● [Re: PayPal's tenuous situation](#)

[Ray Todd Stevens](#)

[Alun Jones](#)

● [Re: The RISK of ignoring permission letters](#)

[Gene Spafford](#)

[Ray Blaak](#)

● [Pearl Harbor Dot Com, by Winn Schwartau](#)

[PGN](#)

● [REVIEW: "Authentication: From Passwords to Public Keys", R.E. Smith](#)

[Rob Slade](#)

● [Info on RISKS \(comp.risks\)](#)

---

## ⚡ Friendly Fire deaths traced to dead battery

Jamie McCarthy <jamie@mccarthy.vg>

*Tue, 26 Mar 2002 10:47:52 -0500*

In one of the more horrifying incidents I've read about, U.S. soldiers and allies were killed in December 2001 because of a stunningly poor design of a GPS receiver, plus "human error."

<http://www.washingtonpost.com/wp-dyn/articles/A8853-2002Mar23.html>

A U.S. Special Forces air controller was calling in GPS positioning from some sort of battery-powered device. He "had used the GPS receiver to calculate the latitude and longitude of the Taliban position in minutes and seconds for an airstrike by a Navy F/A-18."

According to the \*Post\* story, the bomber crew "required" a

"second calculation in 'degree decimals'" -- why the crew did not have equipment to perform the minutes-seconds conversion themselves is not explained.

The air controller had recorded the correct value in the GPS receiver when the battery died. Upon replacing the battery, he called in the degree-decimal position the unit was showing -- without realizing that the unit is set up to reset to its \*own\* position when the battery is replaced.

The 2,000-pound bomb landed on his position, killing three Special Forces soldiers and injuring 20 others.

If the information in this story is accurate, the RISKS involve replacing memory settings with an apparently-valid default value instead of blinking 0 or some other obviously-wrong display; not having a backup battery to hold values in memory during battery replacement; not equipping users to translate one coordinate system to another (reminiscent of the Mars Climate Orbiter slamming into the planet when ground crews confused English with metric); and using a device with such flaws in a combat situation.

---

## **✶ Friendly Fire deaths traced to dead battery**

<knhaw@rockwellcollins.com>

*Tue, 26 Mar 2002 14:35:01 -0800*

[...]

The article states: "Nonetheless, the [anonymous, senior defense department] official said the incident shows that the Air Force and Army have a serious training problem that needs to be corrected. "We need to know how our equipment works; when the battery is changed, it defaults to his own location," the official said. "We've got to make sure our people understand this."

It also states: "...it is not a flagrant error, a violation of a procedure," the official said. "Stuff like that, truth be known, happens to all of us every day -- it's just that the stakes in battle are so enormously high."

[Full article submitted by several others. TNX. PGN]

---

## **British Air Traffic Control system outage**

Alistair McDonald <alistair@inrevo.com>

*Thu, 28 Mar 2002 06:52:50 +0000*

One of the British air-traffic control systems crashed on 27 Mar 2002, and affected airports across Britain. Hundreds of flights were canceled or delayed. A spokesman said that this computer was not connected with the computers at the new Swanwick ATC centre in Hampshire (which opened six years late and millions of pounds over budget). ["connected with" is of course ambiguous in this context. PGN-ed]

<http://uk.news.yahoo.com/020327/80/cvck5.html>

[Simon Waters reported this case also at

[http://news.bbc.co.uk/hi/english/uk/newsid\\_1897000/1897885.stm](http://news.bbc.co.uk/hi/english/uk/newsid_1897000/1897885.stm)

[stm](#)

PGN]

---

## **Clinton cartoon carries virus**

"NewsScan" <newsscan@newsscan.com>

*Wed, 27 Mar 2002 08:17:36 -0700*

McAfee, the anti-virus software company, says a new virus called MyLife.B., is being circulated as an e-mail attachment featuring a cartoon about former president Bill Clinton. A McAfee executive says, "If this one does reach large proportions, it will be a very costly virus because most consumers don't have good backup methods for their operating system or important files on the C drive." The virus e-mails itself to everyone in a user's Microsoft Outlook address book or MSN Messenger contact list. The virus will cause damage only if you open the attachment -- so don't open it! (\*USA Today\*, 26 Mar 2002; NewsScan Daily, 27 March 2002)

<http://www.usatoday.com/life/cyber/tech/2002/03/26/viruses.htm>

---

## **Low-tech election risks: mice**

"Mike Martin" <mike\_martin@altavista.net>

*Wed, 27 Mar 2002 12:58:46 +0900*

Those concerned about the risks of high technology voting methods should remind themselves that low-tech methods (ballot papers marked with a pencil, transported and counted under the watchful eye of scrutineers) present their own risks. \*The Bangkok Post\* reports, [http://www.bangkokpost.com/270302\\_News/27Mar2002\\_news06.html](http://www.bangkokpost.com/270302_News/27Mar2002_news06.html), that, following voting in a by-election on March 3, mice managed to climb into one of the ballot boxes and chew up ballots.

The winning candidate had a 65 vote lead when the undamaged votes were counted, and it was estimated that scraps left by the mice represented another 40 papers. "This result still has to be endorsed by the Election Commission," reports \*The Post\*.

---

## **✶ Black box or Pandora's box?**

Monty Solomon <monty@roscom.com>

*Sun, 24 Mar 2002 17:19:07 -0500*

Black box or Pandora's box?

Most new vehicles come equipped with data recording technology that can help accident investigators. But the computer device has its critics, who fear the overstepping of "Big Brother." [...]

[http://www.phillyburbs.com/intelligencerrecord/article1.asp?F\\_num=1484073](http://www.phillyburbs.com/intelligencerrecord/article1.asp?F_num=1484073)

## **✶ eBay identity theft**

Scott Nicol <sbnicol@mindspring.com>

Wed, 27 Mar 2002 13:13:49 -0500

Interesting article at <<http://zdnet.com.com/2100-1106-868306.html>>.

Summary: You can run a dictionary attack on an eBay account, because eBay doesn't lock an account for invalid logins, no matter how many invalid login attempts are made.

eBay doesn't lock accounts for invalid login attempts because "unscrupulous bidders might try to sabotage their competitors by locking out their accounts or that legitimate users may find themselves unable to log in after an attempted dictionary attack". So I guess identity theft is not as bad as these other possibilities?

Then there's this quote: "We're trying to figure out a way that we can adopt it without disclosing how the process works". It's a pretty simple processes - 3 strikes (or whatever) and you're out. I assume from this quote that they mean they want to implement something that is not so simple, i.e. locking only if it appears to be a dictionary attack. This is security through obscurity - it won't take much time until somebody figures out what constitutes a dictionary attack pattern, then modifies their dictionary attack to avoid the pattern.

Scott Nicol <sbnicol@mindspring.com>

---

## **✶ Software "glitch" changes the colour of the universe**

Pete Mellor <pm@csr.city.ac.uk>

*Wed, 13 Mar 2002 00:35:43 +0000 (GMT)*

As reported on the "Broadcasting House" programme on BBC Radio 4, Sunday 10th March:-

Scientists at John Hopkins University have spent several years calculating the weighted average of the electromagnetic frequency of emissions from all galaxies in the observable universe. They concluded their research by announcing last month that, on average, the universe is turquoise.

Last week, they announced that, due to a software "glitch", they had miscalculated, and that the universe is, in fact, beige.

Broadcasting House are threatening legal action, claiming that they have just had their studio painted turquoise in order to be in harmony with the rest of the universe.

Peter Mellor, Centre for Software Reliability, City University, Northampton Square, London EC1V 0HB UK NEW Tel.: +44 (0)20 7040 8422

---

## **✶ Bioinformatics start-of-the-art**

"Dr Richard A. O'Keefe" <ok@cs.otago.ac.nz>

Wed, 13 Mar 2002 18:26:28 +1300

Bioinformatics is a hot topic at this university, and the computer science department is just starting to get involved. As part of trying to learn about this field, I thought I'd read a couple of the better-known programs. To be honest, I thought I'd run splint (formerly known as lclint) over them and find a minor buig or two. I'm not going to name either of these programs, but one of them was particularly interesting because we were thinking of having a student make a parallel version to try out a parallel architecture one of our people is interested in, because normal runs of this program on recent PCs can take about 3 weeks.

I don't know what art these programs are state-of; possibly macrame.

They certainly aren't even 1970's state of the programming art.

- \* indentation inconsistent, crazy, or both (fix with indent) - lines up
  - to 147 columns wide (fix with indent)
- \* lots of dead variables (fix with quick edit)
- \* array subscripts that could go negative (use unsigned char rather than char in a couple of dozen places, phew)
- \* failure to comprehend that C++ prototypes and C prototypes are different (fix by changing () to (void) in too many places)
- \* #define lint ... so that lint falls over (rename lint to Lint in a dozen files)
- \* assumption that long int = 32 bits (one program) or that int = 32 bits (the other) (not yet done, but use inttypes.h with a local backup)

```
* string->integer code that gets INT_MIN wrong (rip out, plug in
code
  known since 60s)
* using %ld format with int arguments (*printf and *scanf), a
real
  problem because the machines
  (I have access to are 64-biters and it'd be nice if the
programs ran
  in LP64 mode.)
* gcc, liint, splint find variable used before initialised (see
next
  item)
* technically legal syntax with no semantics: double matrix[][]
as
  function argument,. (Scream, bang head on wall, write this
message.)
```

Is it reasonable to expect people with a biochemistry or mathematics background to write clean well-engineered code? No. For the importance of the topic, and the sums of money involved, is it reasonable to expect that they'll have their programs cleaned by someone else before release? I think it is. With the pervasive lack of quality I'm seeing, I don't trust `_any_` of the results of these programs. I have to wonder how many published results obtained using these programs (and fed back into databases that are used to derive more results which are ...) are actually valid.

---

## ⚡ Windows XP disables own firewall

Scott Miller <[scottamiller@usa.net](mailto:scottamiller@usa.net)>  
*Thu, 14 Mar 2002 05:43:05 -0500*

Caveat: this is third hand, I've no way to test. However, the

original

reporter seems to have done sound observation and corroboration, and this

could be important. Extract from a report from Tim Loeb posted on Jerry

Pournelle's mail page ([www.jerrypournelle.com/mail/currentmail.html](http://www.jerrypournelle.com/mail/currentmail.html)):

...What happens is this: either during the initial setup of Earthlink as a

network connection via the Network Connection Wizard or later as an explicit

modification the user attempts to activate XP's Internet Connection

Firewall. All seems to go well. If the user is on-line with the target

connection active at the time he/she will be advised that not all features

can be implemented until sign-off and a fresh log-on. Reviewing the status

of that active connection will show that the check box for Enable Internet

Connection Firewall IS checked, and the user would naturally think the

protection is in place. Running the tests on Steve Gibson's site right then,

with the active connection unbroken since enabling the firewall, will show

that the machine is indeed in full "stealth" mode, and naturally most people

would now assume the issue has been successfully addressed.

WRONG! A fresh

log-on (via Earthlink using their dialer at least - I have no way to test

other ISP connections and/or associated software) DISABLES the firewall, and

the machine is completely open to probes and hacks! I've spent hours testing

this scenario, and the result is always the same: while I can enable the

Internet Connection Firewall and have it work ONCE, as soon as I log off the

network and back on again the protection disappears, and the "enable

Internet Connection Firewall" box reverts to being unchecked.  
Frankly I  
don't know what's happening here, but it is happening on two  
separate  
machines that have never been on a network together...

---

**⚡ Re: LED lights can reveal computer data (Simicich, [RISKS-21.95](#))**

Anthony DeRobertis <asd@suespammers.org>  
*Wed, 13 Mar 2002 22:17:53 -0500*

My Lego Mindstorms set communicates with both infrared and  
visible LED's. So  
does your television remote control. And many other things.

If you want to communicate with LEDs, you can. However, I doubt  
very much  
that it is easy to read data passing over a modem from the  
activity light!  
Unless it only lights for, e.g., 1's. Even then, at reasonable  
data rates  
--- especially since you have no ECC coding or even clock sync  
--- it seems  
nearly impossible.

---

**⚡ Re: Disclaimers (Bacon, [RISKS-21.95](#))**

Malcolm Cohen <malcolm@nag.co.uk>  
*Wed, 13 Mar 2002 11:15:21 +0000 (GMT)*

>... "Was the original e-mail monitored - WITHOUT the  
recipient's consent?"

The recipient has nothing to do with it. It is the sender who

has copyright  
on the email (the recipient is not entitled to publish it).

Just like letters and other "ordinary" correspondence, the sender can show it to anyone else. Obviously, by choosing to use a monitored email system, he has chosen to let it be monitored.

>How long before the 'thought police' in the BBC extend their monitoring...

Well, actually, it is normal company policy at most places to open all incoming correspondence (e.g. letters) as a matter of course! And it's not unheard of for certain companies (e.g. mail-order ones) to record all telephone calls as a matter of course.

And how you imagine that postcards and faxes are "not examined" by anyone involved with the delivery, I don't know! They have to start reading the thing to see who to give it to, it's human nature to look at the rest.

Use of company phones (some places run a "no private calls" policy), company fax machines, and the company mail service is obviously all down to company policy. Why one would imagine that these things are provided for the personal benefit of employees rather than to conduct company business, I don't know.

As long as the employees know what the policy is I see no grounds for complaint (other than to grumble about the policy being strict).

Malcolm Cohen, NAG Ltd., Oxford, U.K. (malcolm@nag.co.uk)

## ✦ **Re: PayPal's tenuous situation (Max, [RISKS-21.94](#))**

"Ray Todd Stevens" <raytodd@kiva.net>

*Wed, 13 Mar 2002 11:04:32 -5*

I use PayPal from the vendor side, and I can assume you that you did not quite understand the system. Actually, most people I know of who make extensive use of PayPal end up with a "fraud investigation hold" on their accounts from time to time. PayPal seems to have a system that monitors transactions for weird activity and automatically puts such a hold on accounts. Then it appears that a human reviews the activity and investigates. If you recieve a drastic increase in the number of transactions you get flagged. What got me was having money arrive and then immediately sent somewhere else. So a fraud hold does not mean that there is fraud, but that there appears there may be.

A fraud hold does mean that you don't have access to the funds coming in. You can not issue bills to people. (That is, you can't use the PayPal system to ask people to pay you.) More important, a person with a fraud hold can't access the funds. They can issue refunds, but may not send the money to other people. They also may not withdraw funds. This means that PayPal probably has your money and you will get it back. It also means that, if their automatic system flags your account, you can continue to do business for the period of time the investigation takes. In my case one hold was about 2 hours and another was about 8 hours.

I hope this helps you and the group understand this system better.

Ray Todd Stevens, Senior Consultant, Stevens Services, Suite 21  
3754 Old State Rd 37 N, Bedford, IN 47421 1-812-279-9394  
Raytodd@kiva.net

---

**Re: PayPal's tenuous situation (Bayley, [RISKS-21.94](#))**

Alun Jones <alun@taxis.com>

*Tue, 12 Mar 2002 20:26:35 -0600*

As a merchant myself, accepting credit cards for some time, I can state quite categorically (and with some rancour) that the approval from the credit-card company is by no means whatsoever a guarantee of payment. It provides a merchant with pretty close to no protection at all. I've been provided with chargebacks (which are automatically deducted from my business' accounts) on transactions where I have meticulously verified that the credit-card company gave me authorisation.

As far as I can make out, the only "guarantee" is that the checksum matches, the card hasn't expired through old age, and probably hasn't been reported as stolen any time longer than a week ago.

Oh, and chargebacks may get submitted to you many months after the original purchase. I had one bank try to process a chargeback about two years after the original purchase. The number of chargebacks submitted

works against you, as well, as the credit-card company will increase your "discount rate" (the percentage of the transaction that they take from you) if you have too many. Is this to cover their expenses in handling those chargebacks? Why, no, of course not. After all, every chargeback is not only charged at that same discount rate both coming and going, but also has the helpful addition of a "service charge" of \$25 added on for your convenience.

For as much as credit-card holders may feel concerned about whether their money is safe in an online transaction (in the USA, law requires it to be so), the merchants are always the ones left holding the bag.

Texas Imperial Software, 1602 Harvest Moon Place, Cedar Park TX  
78613-1419  
Fax/Voice +1(512)258-9858

---

## **✶ Re: The RISK of ignoring permission letters (Knox, [RISKS 21.94](#))**

Gene Spafford <spaf@cerias.purdue.edu>  
*Tue, 12 Mar 2002 21:57:30 -0500*

I have a fairly simple response to spam e-mail that claims I requested it, or can only opt out, or whatever.

I determine the actual sending address, and the domain of any associated URLs in the message, and I add them to my "black hole" list. Any future mail from that address is bounced. Domains that offer repeated abuses are

added, too. E-mail in languages other than English with embedded prices, porno, or URLs to commerce sites automatically go into the list. I also have added addresses collected in like manner by several friends; I have not used any of the major anti-spam sites (yet).

It doesn't matter what they claim -- I no longer see their spam.

Based on a multi-year history of e-mail, I now completely block any e-mail from msn.com, any version of yahoo.com, and hotmail.com --- I have had (literally) thousands of spam messages from there, but only 6 legit correspondents. I am also blocking 3200 separate addresses and over 6400 other domains.

My spam load is down to only about 10-15 new pieces per day. :-)

And by the way, if this is being read by the pinheads who keep sending out ads for reconditioned printer cartridges, please know that we will *\*never\** do business with your firms. We're keeping a list.

---

**✶ Re: The RISK of ignoring permission letters (Slade, [RISKS-21.95](#))**

Ray Blaak <blaak@telus.net>  
*Thu, 14 Mar 2002 04:39:16 GMT*

> Does a failure to respond to this type of message constitute a legitimate  
> "acceptance" on my part? (Particularly for those of us from outside the US?)

This can't be right. So, if the e-mail is lost in cyberspace and you never even receive it, is that the same as implicitly consenting?

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.

---

## ✈ Pearl Harbor Dot Com, by Winn Schwartau

"Peter G. Neumann" <neumann@csl.sri.com>  
*Sun, 24 Mar 2002 16:36:15 PST*

Pearl Harbor Dot Com  
A novel by Winn Schwartau  
Interpact Press  
Seminole, Florida, 1-727-393-6600  
2002  
ISBN 0-9628700-6-4  
512 pages

We do not normally review or analyze RISKS-relevant fiction, but this book seems to make a rather compelling novel out of a surprisingly large number of security and reliability risk threats that we have discussed here over the years. The story echoes one of the fundamental problems confronting Cassandra-like risks-avoidance protagonists and agonists alike, namely, that, because we have not yet had the electronic Pearl Harbor, people in power perceive that there is little need to fix the infrastructural problems, so why bother to listen to the doom-sayers who hype up

the risks?

Well, in this novel, one man's massive craving for vengeance reaches major proportions, and significant effects result on critical infrastructures. In the end, the good hackers contribute notably to the outcome.

The book is somewhere within the genre of technothrillers, with a typical mix of murder, mayhem, intrigue, computer-communication surveillance, and non-explicit s\*x. I enjoyed it. It is entertaining, and the convoluted plot is quite consistent, fairly tight, and to RISKS readers, each incident is technologically quite plausible -- because many of the attacks seem almost reminiscent of past RISKS cases, sometimes just scaled up a little.

If you read the book, try not to let the sloppy proof-reading bother you; there are too-frequent typos and grammar glitches, and lots of misspellings -- for example, Naugahyde is subjected to two different versions, each with at least two letters wrong, and Walter Reade is misspelt twice, differently, on the same page! Incidentally, the author and his previous writings make several self-referential appearances throughout the story, which might seem rather self-serving, but does draw attention to the author's long-standing role in trying to combat what has now become known as cyberterrorism.

---

**⚡ REVIEW: "Authentication: From Passwords to Public Keys", R. E. Smith**

Rob Slade <rslade@sprint.ca>

Mon, 18 Mar 2002 11:57:50 -0800

BKAUTHNT.RVW 20020220

"Authentication: From Passwords to Public Keys", Richard E. Smith,

2002, 0-201-61599-1, U\$44.99/C\$67.50

%A Richard E. Smith

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

M3C 2T8

%D 2002

%G 0-201-61599-1

%I Addison-Wesley Publishing Co.

%O U\$44.99/C\$67.50 416-447-5101 fax: 416-443-0948 bkexpress@aw.com

%P 549 p.

%T "Authentication: From Passwords to Public Keys"

Chapter one looks at the history and evolution of password technology, and introduces a system of discussing attacks and defences that provides an easy structure for an end-of-chapter summary. A more detailed history appears in chapter two, while chapter three discusses the enrolling of users.

Chapter four is rather odd: it brings up the concept of "patterns" as defined in the study of architecture, but doesn't really explain what this has to do with authentication or the book itself. The closest relation seems to be the idea of determining a security perimeter. The material poses a number of authentication problems and touches on lots of different technologies, but the various difficulties are not fully analyzed.

Chapter five is supposed to be about local authentication, but

mostly  
examines encryption.

Strangely, chapter six inveighs against the complex rules for password choice and management that are commonly recommended--and then adds to the list of canons the requirement to assess the security of a system when choosing a password. Ultimately the text falls back on the traditional suggestions, with a few good suggestions for password generation. This place in the text also marks a change in the volume: the content moves from a vague collection of trivia to a much more practical and useful guide.

Chapter seven is a decent overview of biometrics, although there is an odd treatment of false acceptance and rejection rates, and some strange opinions. Authentication by address, emphasizing IP spoofing, is covered in chapter eight, while hardware tokens are discussed in chapter nine. Challenge/response systems are reviewed in chapter ten, as well as software tokens. Indirect or remote authentication, concentrating on the RADIUS (Remote Authentication Dial In User Services) system, is examined in chapter eleven. Chapter twelve outlines Kerberos, and has a discussion of the Windows 2000 version, albeit with limited analysis. The study of public key (asymmetric) cryptography in chapter thirteen would be more convincing with just a few more sentences of explanation about how keys are established. Chapter fourteen talks about certificates and signing, while fifteen finishes with some vague thoughts on password storage.

After a slow (but interesting) start, the book does have a good deal of useful material in the later chapters. Long on verbiage and

a bit

short on focus, this text does have enough to recommend it to security

practitioners serious about the authentication problem.

copyright Robert M. Slade, 2002 BKAUTHNT.RVW 20020220

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](#)